Pace Law Review

Volume 30
Issue 2 *Winter 2010*

Article 20

January 2010

"Intelligence" Searches and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence-Gathering

Robert C. Power
Widener University School of Law

"Intelligence" Searches and Purpose: A Significant Mismatch Between Constitutional Criminal Procedure and the Law of Intelligence-Gathering

Robert C. Power*

Hassan Abu-Jihaad, a United States citizen who served in the U.S. Navy for about four years, was indicted in 2007 for providing information to a terrorist group via email and the internet.[1] In particular, Abu-Jihaad was charged with sending classified information about a U.S. Navy Battle Group scheduled for deployment in the Persian Gulf region in 2001.[2] Separate counts charged providing material support to a conspiracy to kill U.S. nationals and communicating national defense information to persons not entitled to receive it.[3]

While the charges were pending, the government filed notice of its intention to use evidence derived from national security electronic surveillance.[4] Abu-Jihaad's counsel moved

* Associate Dean for Faculty Research and Development and Professor of Law, Widener University School of Law. Dean Power thanks John Dernbach, Andrea Nappi, Ed Sonnenberg, and Bonnie Lerner for their help in researching and writing this article. Power served as the H. Albert Young Fellow in Constitutional Law from 2007 to 2009 and thanks the Young Foundation and the Young family for their support of this article and several other research projects on constitutional law and human rights.

1. Indictment, United States v. Abu-Jihaad, 2007 WL 4961131, at ¶¶ 1, 12-27 (D. Conn. Mar. 5, 2008) (No. 07CR57), 2007 WL 4961131.

2. *Id.* ¶¶ 21, 25, 31.

3. *Id.* ¶¶ 28-31. The providing material support count was charged under 18 U.S.C. § 2339A (2006), *id.* ¶ 29, and the communicating national defense information count was charged under 18 U.S.C. § 793(d) (2006), *id.* ¶ 31.

4. Amended Notice of Intention to Use Foreign Intelligence Surveillance Act Information Pursuant to 50 U.S.C. §§ 1806(c), 1825(d), United States v. Abu-Jihaad, 2008 WL 676037 (D. Conn. Mar. 5, 2008) (No.07CR57). *See* Motion to Suppress FISA Derived Evidence, United States v. Abu-Jihaad, 2008 WL 676037 (D. Conn. Mar. 5, 2008) (No. 07CR57), 2007 WL 4961126, at ¶ 2 (discussing the Government's Motion).

to suppress that evidence but found his hands tied because he was not permitted to view either the legal documents in support of the government's electronic surveillance application or the orders of the Foreign Intelligence Surveillance Court ("FISC") issued in reliance on those documents.[5] The defense motion was in some respects similar to shadowboxing, as arguments were necessarily presented on the basis of assumptions and guesses about the nature of the government's investigation and the strength of its case against Abu-Jihaad and his unindicted co-conspirators.[6] The trial judge denied Abu-Jihaad's request for information about the surveillance, examined the documents *in camera*, and upheld the use of the evidence in the criminal trial.[7] Abu-Jihaad was convicted of both charges in 2008.[8] In 2009, the judge upheld the conviction for providing classified information and granted a judgment of acquittal on the material support charge.[9]

Several years before Abu-Jihaad's conviction, FBI agents assisting Spanish authorities who were themselves investigating the March 2004 Madrid train-bombing, focused attention on an Oregon attorney, Brandon Mayfield.[10] A fingerprint was recovered on items used in the bombing, and FBI analysis determined it to be similar to 20 fingerprints which the FBI had on file in its Automated Fingerprint Identification System ("AFIS").[11] Mayfield's "adherence to the

---

5. Motion to Suppress FISA Derived Evidence, *supra* note 4, at ¶ 3. *See also infra* note 80 (discussing the FISC).

6. *See* Memorandum in Support of Motion to Suppress FISA Derived Evidence, United States v. Abu-Jihaad, 2008 WL 676037 (D. Conn. Mar. 5, 2008) (No 07CR57), 2007 WL 4961127. For example, counsel tried to make an argument under *Franks v. Delaware*, 438 U.S. 154 (1978), that the government's applications contained false information about the classified nature of some of the information in question, but was unable to point to specific assertions in the applications and argue that they were recklessly false. *Id.*

7. United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 301 (D. Conn. 2008).

8. Jury Verdict, United States v. Abu-Jihaad, 2008 WL 676037 (D. Conn. Mar. 5, 2008).

9. United States v. Abu-Jihaad, 600 F. Supp. 2d 362, 365 (D. Conn. 2009).

10. *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1027 (D. Or. 2007), *vacated*, 588 F.3d 1252 (9th Cir. 2009).

11. *Id.*

Muslim faith,"[12] led the FBI to conduct electronic surveillance at Mayfield's home and law office, and to execute surreptitious searches of both locations.[13] Mayfield was later subjected to material witness proceedings, arrest, incommunicado custody, and pressure to confess.[14] The fingerprint was later matched to an Algerian man who was apparently involved in the terrorist bombings, and Mayfield was exonerated.[15]

Mayfield was far more fortunate than Abu-Jihaad. His custody was short, and he received a substantial settlement for most of his claims against the government.[16] Still, United States citizens suspected of terrorist activities, or even involvement with foreign organizations, can take little comfort from this story.[17] The settlement did not resolve Mayfield's

---

12. *Id.* at 1027.

13. *Id.* at 1029.

14. *See id.*

15. *Id.*

16. *Id.* at 1026. *See, e.g.*, Ryan Geddes, *Mayfield Settles Case Against Feds for $2 Million*, BEAVERTON VALLEY TIMES, Nov. 29, 2006, *available at* http://www.beavertonvalleytimes.com/news/story.php?story_id=11648268729 1016800; Eric Lichtblau, *U.S. Will Pay $2 Million to Lawyer Wrongly Jailed*, N.Y. TIMES, Nov. 30, 2006, at A18; Henry Schuster & Terry Frieden, *Lawyer Wrongly Arrested in Bombings: 'We lived in 1984'*, CNN.COM, Nov. 30, 2006, http://www.cnn.com/2006/LAW/11/29/mayfield.suit/index.html.

17. There are obviously many other intriguing stories about the treatment of U.S. citizens and others in the United States and elsewhere during the war on terrorism. One intriguing story involved Cyrus Kar, who was taken into custody by the United States military in Iraq in 2005. *See* Kar v. Rumsfeld, 580 F. Supp. 2d 80, 81-82 (D.D.C. 2008). An American citizen working on a documentary film, Kar and his Iraqi cameraman were traveling in a Baghdad taxi when they were stopped by Iraqi police. *Id.* at 81. Kar was promptly transferred to U.S. military custody, where he was held for over seven weeks, most of that time in solitary confinement, in harsh conditions, at a military detention center. *Id.* at 82. At one point Kar was interrogated by an FBI agent. *Id.* According to the district court's written opinion in Kar's civil case against the government, "[w]hen he asked the agent if he could speak with an attorney, the agent laughed and replied that none were available. The agent added that Kar had the right to remain silent, but he said that the last person to exercise that right was still being detained in Afghanistan two years later." *Id.* Kar agreed to talk, submitted to a polygraph examination, and consented to a search of his home in California. *Id.* A status hearing pursuant to the Geneva Conventions was held on short notice. *Id.* The hearing officers concluded that Kar was innocent, and he was released six days later. *Id.* at 82-83. A federal district court later dismissed a damages action that Kar brought against the government, largely on the basis of qualified immunity. *Id.* at 86. While the court concluded that, as a United States citizen, Kar was protected by the Fourth and Fifth Amendments—even while abroad in a war zone—and that

claim that an amendment to the Foreign Intelligence Surveillance Act ("FISA")[18] violated the Fourth Amendment.[19] Related arguments claimed that covert physical searches authorized by amendments to FISA similarly violated the Fourth Amendment.[20] Mayfield prevailed in the district court,[21] but most other challengers to those provisions have failed, including Abu-Jihaad.[22] As a result, even American citizens in the United States are likely to remain subject to tactics more conducive to war than to criminal investigation. This is true, even though, as in *Mayfield* and possibly in *Abu-Jihaad*, the government is investigating a past criminal act. Moreover, even if the courts reverse direction and follow the *Mayfield* court's approach, victims will not be remedied until their rights are clearly established,[23] something that is not

---

he had been denied some of those rights by this treatment, those rights were not clearly established in law, and therefore, the court could not support an award of damages. *Id.* at 84-86. The court's ruling illustrates some of the difficulties of enforcing constitutional rights abroad and during wartime. While the court in *Kar* concluded that the initial arrest and detention were lawful under war conditions, but that the delay of forty-eight days from Kar's arrest to his probable cause hearing exceeded constitutional limits, the court was unable to conclude that there had been a violation of a clearly established right to a prompt probable cause hearing under combat conditions. *Id.* at 84-85. The result of the case was judicial recognition that, even for a United States citizen arrested several years into the occupation of Iraq, nothing resembling the rights recognized in the criminal justice system could legitimately be imposed on the military's efforts to conduct the war on terror within a war zone.

18. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

19. *See Mayfield*, 504 F. Supp. 2d at 1030.

20. *Id.* at 1030-33 (discussing the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 218, 115 Stat. 272, 291 (codified as amended at 50 U.S.C. §§ 1804, 1823). Mayfield argued that the USA-PATRIOT Act's FISA amendments allow the government to "avoid the Fourth Amendment's probable cause requirement when conducting surveillance or searches of a criminal suspect's home or office merely by asserting a desire to also gather foreign intelligence information from the person whom the government intends to criminally prosecute." *Id.* at 1032.

21. *Id.* at 1042-43. The decision, however, was vacated and remanded by the Ninth Circuit due to Mayfield's lack of standing. Mayfield v. United States, 588 F.3d 1252 (9th Cir. 2009).

22. *See* United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 304 (D. Conn. 2008) (expressly rejecting the holding in *Mayfield*).

23. A major obstacle to civil relief for claims of Fourth Amendment violations in this arena is the fact that qualified immunity will prevent recovery unless the right is clearly established at the time the alleged

even on the horizon nearly a decade after the beginning of the War on Terror.

The last twenty years have seen a dramatic expansion of military and civilian efforts against international terrorism. Every few years, legislation has tweaked the federal criminal code or intelligence laws to make it easier to identify and incarcerate terrorists. Much of this legislation has been appropriate, especially in light of new technology that has made it more difficult to collect intelligence and evidence against foreign agents. Other legislative acts, however, have created more problems than they seem to have solved.

President George W. Bush's first Attorney General, John Ashcroft, announced the "New Paradigm" soon after September 11, 2001.[24] This was a change in the Department of Justice's ("DOJ") mission from prosecution of criminals to prevention of terrorism.[25] In the name of anti-terrorism, many of the Bush administration's efforts expanded law enforcement's powers to act.

The constitutional doctrine that existed prior to this shift in emphasis may not be enough to protect the public as the founders had intended. While some judicial decisions and legal trends are responsive to expanded government powers, such as the extraterritorial application of Fourth and Fifth Amendment rights, others are less so. This would include the apparent

---

violation occurred. *See* Kar v. Rumsfeld, 580 F. Supp. 2d 80, 83-84 (D.D.C. 2008) (citing Saucier v. Katz, 583 U.S. 174, 201 (2001)).

24. *See* JOHN ASHCROFT, NEVER AGAIN: SERVING AMERICA AND RESTORING JUSTICE 124-26, 133 (2006) (describing a need for new infrastructure and a culture of preventing terrorism rather than prosecuting terrorist crimes). *See also infra* note 25.

25. John Ashcroft, United States Attorney General, Speech before Council on Foreign Relations (Feb. 10, 2003), http://usinfo.org/wf-archive/2003/030210/epf116.htm ("In order to fight and to defeat terrorism, the Department of Justice has added a new paradigm to that of prosecution—a paradigm of prevention."). *See also* JANE MAYER, THE DARK SIDE 33 (2008); David Cole, *Are We Safer?*, 53 N.Y. REV. OF BOOKS 4 (2006), http://www.nybooks.com/articles/18752 (reviewing DANIEL BENJAMIN & STEVEN SIMON, THE NEXT ATTACK: THE FAILURE OF THE WAR ON TERROR AND A STRATEGY FOR GETTING IT RIGHT (2006)) ("Within the US, Attorney General John Ashcroft repeatedly promoted what he labeled a new 'paradigm of prevention' in law enforcement."); Tillie Fong, *Ashcroft Defends the Patriot Act*, ROCKYMOUNTAINNEWS.COM, Nov. 28, 2007, http://www.rockymountainnews.com/news/2007/nov/28/ashcroft-defends-the-patriot-act/.

green light that Congress has given the government to use intelligence tools to investigate criminal activity, as identified in *Mayfield*.[26]

This Article addresses the role of constitutional criminal procedure in national security investigations, focusing on the role of government's *purpose* in taking action. This is the key question, given Ashcroft's redirection of the Department of Justice. The same tools are used in both criminal and intelligence investigations. If the government searches a home or conducts electronic surveillance, it intrudes on the same privacy interests and learns the same type of data—physical evidence that is located in the home or words that are spoken in the vicinity of a microphone. What differs is the government's purpose—the reason for taking the action. Purpose inquiries are critical to this issue because it is the purpose of the investigation that determines the applicable law. Here, a subtle part of the USA-PATRIOT Act and its amendments to FISA have had a major impact, as considered by the courts in *Abu-Jihaad* and *Mayfield*. This Article therefore examines FISA, with particular attention to the 2001 amendments, to determine if the distinction between a criminal investigatory purpose and a foreign intelligence purpose can and should be dispositive of Fourth Amendment issues. Most courts have concluded that the change was appropriate, but this Article argues that, under a totality of the circumstances approach consistent with Fourth Amendment analysis generally, the courts have overlooked both the significance of the change and the fact that it has created an easy road to conduct extraordinarily intrusive warrantless searches without probable cause. It would be too strong to say that the 2001 amendments were a paving stone on the road to the hell of a police state—but it would not be too much to say that they permit the government to play bait-and-switch with the courts in a fashion that denigrates constitutional rights without any apparent gain in serving national security.

26. *See* 504 F. Supp. 2d at 1027.

I. FISA and the Expansion of National Security Surveillance

A. *The Landscape in 1978*

The central legal authority concerning intelligence collection is FISA, which was enacted in 1978.[27] FISA was passed following Senate hearings on abusive practices in the United States and abroad by the CIA.[28] The hearings fed a national belief that executive discretion in the field of intelligence required greater oversight. FISA was also, in large part, a response to the Supreme Court's decision in *United States v. United States District Court* (Keith).[29] *Keith* presented the executive branch with a mandate to conform its domestic actions to the Fourth Amendment.[30]

1. *Keith*

The *Keith* decision involved the warrantless electronic surveillance of Robert Plamondon, a defendant in a federal prosecution of radicals for destruction of government property.[31] The government acknowledged that Plamondon

27. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

28. The Senate Report to FISA referred at length to the abuses uncovered in Senate hearings chaired by Frank Church of Idaho and to the case law of the time, including *Keith*. S. REP. NO. 95-604 (pt. I), at 7-15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908-16. For a good history of intelligence actions by United States agencies, including the CIA leading up to the Church Committee hearings, see Seth Kreimer, *Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror*, 7 U. PA. J. CONST. L. 133 (2004). *See also generally* Richard Henry Seamon, *Domestic Surveillance For International Terrorists: Presidential Power and Fourth Amendment Limits*, 35 HASTINGS CONST. L.Q. 449 (2008) (placing unilateral executive actions in historical and constitutional perspective); James G. McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, U.S. DEP'T OF HOMELAND SEC., March 2007, http://www.fletc.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/foreign-intelligence-surveillance-act.html/.

29. United States v. United States Dist. Court (*Keith*), 407 U.S. 297 (1972). All justices participating in the decision agreed with the outcome. Justice Rehnquist, who had recently served in the Department of Justice, recused himself.

30. *See id.*

31. *Id.* at 299. *Keith* is addressed in several recent articles on FISA and related issues. *See, e.g.*, Tracey Maclin, *International Crime and Terrorism:*

had been subject to warrantless electronic surveillance, but argued that it was authorized by Title III of the Omnibus Crime Control Act ("Title III"),[32] which regulated federal and state use of electronic surveillance.[33] The technical issue was whether language in Title III that indicated that the statute did not limit any presidential power to protect national security had the effect of giving the President the power to conduct electronic surveillance directed against domestic groups that advocated violence against the government.[34] The Court concluded that "Congress simply left presidential powers where it found them,"[35] neither adding to them, as argued by the government, nor taking away from them.[36] This was, in essence, a decision based on plain-meaning statutory interpretation. The Court stressed the limits of its analysis,

---

The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons From Justice Powell and the Keith *Case*, 41 U.C. DAVIS L. REV. 1259, 1279-92 (2008); Dan Fenske, Comment, *All Enemies, Foreign and Domestic: Erasing the Distinction Between Foreign and Domestic Intelligence Gathering Under the Fourth Amendment*, 102 NW. U. L. REV. 343, 353-55 (2008). For contemporary readings of *Keith*, see United States v. Butenko, 494 F.2d 593, 601-02 (3d Cir. 1973); United States v. Brown, 484 F.2d 418, 425-26 (5th Cir. 1973).

32. The Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211-25 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2006)).

33. *Keith*, 407 U.S. at 300.

34. The language in question stated:

> Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. 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 against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.

82 Stat. at 214, 18 U.S.C. § 2511(3) (1970), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1783, 1797.

35. *Keith*, 407 U.S. at 303.

36. *Id.* at 302-08.

noting that the case did not concern the President's powers concerning foreign actions occurring "within or without this country."[37]

The opinion was classic "Justice Powell":[38] it was cautious, it tried to follow a middle course, and it purported to be fact-bound even as it discussed side or unnecessary issues. The discussion of presidential power led to a discussion of legitimate concerns about electronic surveillance and the important role that the Fourth Amendment plays due to the substantial impact that electronic surveillance has on privacy.[39] This typical judicial balancing of legitimate public values against the impact on civil liberties then led to the Court's explanation of why a warrant requirement is constitutionally required: "These fourth amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[40]

The Court addressed the question of the purpose of a government search for intelligence information in an unremarkable discussion of arguably applicable Fourth Amendment exceptions. The Court described the purpose of the electronic surveillance directed at Plamondon as "the

37. *Id.* at 308. The Court both confronted the fact that all post-World War II presidents had asserted the power to use electronic surveillance against domestic subversives, and it recognized the value of electronic surveillance to legitimate government investigations. *Id.* at 310-11 & n.10.

38. Justice Powell's attempt to forge a path between constitutional absolutes is acknowledged in numerous commentaries. *See, e.g.*, Paul R. Baier, *Of* Bakke*'s Balance,* Gratz *and* Grutter*: The Voice of Justice Powell*, 78 TUL. L. REV. 1955 (2004); Paul W. Kahn, *The Court, the Community and the Judicial Balance: The Jurisprudence of Justice Powell*, 97 YALE L.J. 1 (1987); Craig Evan Klafter, *Justice Lewis F. Powell, Jr.: A Pragmatic Relativist*, 8 B.U. PUB. INT. L.J. 1 (1998); Sandra Day O'Connor, *A Tribute to Justice Lewis F. Powell, Jr.*, 101 HARV. L. REV. 395 (1987); Mark Tushnet, *Justice Lewis F. Powell and the Jurisprudence of Centrism*, 93 Mich. L. Rev. 1854 (1995).

39. *Keith*, 407 U.S. at 312-13. The opinion also notes the fact that national security cases tend to challenge First Amendment values, as the line between legitimate political dissent and illegitimate political subversion is vague. *Id.* at 313. This concern became codified in FISA. *See infra* note 85.

40. *Id.* at 316-17. As in *Katz v. United States*, 389 U.S. 347 (1967), which was then and is still today, the central decision on the meaning of "search" under the Fourth Amendment, the Court noted that the electronic surveillance conducted against Plamondon might have been reasonable under the facts, but that this was not sufficient—prior judicial authorization was required under the Fourth Amendment. *Id.* at 317-18.

collecting and maintaining of intelligence with respect to subversive forces, and . . . not an attempt to gather evidence for specific criminal prosecutions."[41] The Court rejected the government's argument that this motivation either rendered the Fourth Amendment inapplicable or permitted unilateral executive branch action.[42] The Court's reasoning provided some direction for resolving present-day problems. "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[43] Thus, an intelligence, rather than a law enforcement purpose, did not convince eight justices in 1972 that a non-law enforcement purpose—even such a compelling one as preventing violence by subversive groups—was sufficient to justify doing away with traditional Fourth Amendment protections.

Keith necessarily left gaps in the constitutional law of intelligence-gathering. First, and most obviously, the warrant requirement it imposed did not extend, at least on its own terms, to cases involving foreign intelligence. The opinion ended by reiterating that the warrant requirement applied only to "domestic aspects of national security," without fully defining the category, other than to state that the ruling did not apply to "foreign powers or their agents."[44] Second, the opinion emphasized that electronic surveillance for domestic intelligence might be appropriate under different standards than those that apply to criminal law enforcement, noting both its own use of constitutional interest balancing for non-law enforcement searches, as well as the propriety of congressional action to establish reasonable standards.[45] Thus, *Keith* seemed

41. *Id.* at 318-19.

42. *Id.* at 319-20.

43. *Id.* at 320. The Court concluded that courts are sufficiently knowledgeable about national security and are not too insecure to handle such important matters. *Id.* It characterized the adverse impact on the executive branch of a warrant requirement as simply a minor added "inconvenience." *Id.* at 321.

44. *Id.* at 321-22 & n.20.

45. *Id.* at 322-23. The Court specifically quoted *Camara v. Municipal Court*, which had applied the Fourth Amendment's warrant clause to administrative inspections, and which had utilized justifications that were different in kind and degree from probable cause. *Id.* at 323 (quoting Camara v. Mun. Court, 387 U.S. 523, 534-35 (1967)). This can be seen as an early reference to the category that later became known as "special needs"

to acknowledge the existence of three categories of searches: criminal law enforcement searches, including electronic surveillance as authorized by Title III;[46] foreign intelligence searches, which might be immune from the warrant requirement and which were (then) ungoverned by federal statutory law;[47] and domestic intelligence searches, such as that which was directed at Plamondon, and which were fully subject to the Fourth Amendment.[48] At least in the absence of statutory provisions authorizing domestic security searches and electronic surveillance, presumably the traditional Fourth Amendment requirements applied to such searches.

Several lower courts decided in the 1970s to accept the *Keith* Court's invitation to recognize a presidential power to conduct searches against "foreign powers."[49] Although the Supreme Court never accepted any of these decisions for review, it is fair to conclude that the general approval of this theory represented a consensus that "foreign intelligence" cases were different, although there was no uniform understanding of all of the defining factors differentiating domestic from foreign cases. This became relatively unimportant because FISA was enacted in 1978, and it became the primary authority, rather than the negative-pregnant implications of the *Keith* decision. Still, one case involving pre-FISA electronic surveillance for foreign intelligence purposes is worth discussing, both because it has received substantial attention over the years and because it seems to be the origin of the key factor in differentiating foreign intelligence searches from other searches—the primary purpose test.

United States v. Truong, decided in 1980, after FISA had been enacted, concerned electronic surveillance and physical

---

searches. *See infra* Part II(A).

46. 407 U.S. at 306.

47. *See id.* at 308-09.

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

49. *See, e.g.*, Jabara v. Kelley, 476 F. Supp. 561, 575-77 (E.D. Mich. 1979), *vacated*, 691 F.2d 272 (6th Cir. 1982), *cert. denied*, 464 U.S. 863 (1983); United States v. Buck, 548 F.2d 871, 875-76 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1977); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974); United States v. Butenko, 494 F.2d 593, 602-06 (3d Cir. 1973), *cert. denied*, 419 U.S. 881 (1974). *But cf.* Chagnon v. Bell, 642 F.2d 1248, 1259 n.17 (D.C. Cir. 1980), *cert. denied*, 453 U.S. 911 (1981) (noting that prior decisions invalidating domestic intelligence operations did not invalidate foreign intelligence operations).

searches that had been conducted in 1977 and 1978, prior to the final congressional action on FISA.[50] The case addressed several months of electronic surveillance of Truong's telephone and his apartment, all conducted without court authorization.[51] The Fourth Circuit upheld the lower court's decision to admit evidence from the first several weeks of the electronic surveillance, but it suppressed the rest.[52] Warrantless electronic surveillance during the first time period was permissible because the court agreed that there was inherent executive power to conduct foreign intelligence surveillance.[53] At least two limitations served to prevent executive abuse of its powers in this area. First, the court limited the power to conduct warrantless electronic surveillance to situations where "the object of the search or the surveillance is a foreign power, its agent or collaborators."[54] Second, the court affirmed the district court's conclusion that the executive power extends only so long as "the surveillance is conducted 'primarily' for foreign intelligence reasons."[55] This distinction was rooted in both competency and theoretical reasons: courts, rather than administrative officials, are the experts and appropriate bodies to evaluate the justification for criminal investigative techniques.[56] At the same time, privacy concerns typical of Fourth Amendment analysis eclipse international policy concerns once the government is working toward a criminal prosecution.[57] The court did not try to split the hairs any more finely—a search was either primarily intelligence or primarily criminal, and this categorization would determine the appropriate standards for authorization. In a brief concluding

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

51. *Id.* at 912.

52. *Id.* at 913, 931.

53. The court interpreted *Keith* as acknowledging executive power in this realm, finding that the policies the Supreme Court held not to be prevailing in the arena of domestic intelligence were sufficiently convincing in the area of foreign intelligence. *Id.* at 913-15. These policies include executive expertise in international relations and the relative lack of knowledge by judges. *Id.* at 913-14.

54. *Id.* at 915.

55. *Id.*

56. Here the court, to some extent, jumps to the conclusion that probable cause is the key factor once a search occurs in a criminal investigation. *See id.*

57. *Id.*

section that provided guidance for later developments, the court addressed the facts indicating the shift in the Truong investigation. Prior to July 20, 1977, the matter had been an intelligence investigation.[58] At that time, however, the Criminal Division of the Justice Department clearly took charge of the investigation as it began to structure a criminal prosecution.[59] Thus, in the case that most fully considered the scope of governmental powers concerning foreign intelligence prior to FISA, the purpose of the search or surveillance was the critical factor in determining the applicable law.

2. FISA

FISA largely tracked the *Keith* and *Truong* analysis by providing a legal structure for several different varieties of electronic surveillance.[60] Some forms of electronic surveillance were to remain exempt from judicial oversight. Thus, Section 102 of the FISA statute provided generally that the President could authorize electronic surveillance without a court order when the surveillance is directed at communications of foreign powers and "there is no substantial likelihood" of intercepting the communications of any United States citizen or permanent resident.[61] The several definitions of "electronic surveillance"

---

58. *See id.* at 915.

59. *Id.* at 916.

60. Numerous articles detail FISA and its history. *See, e.g.*, Adam Burton, *Fixing FISA For Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381, 386-89 (2006); Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity For Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF., 145, 147-51 (2007); Richard Henry Seamon, *Domestic Surveillance For International Terrorists: Presidential Power and Fourth Amendment Limits*, 35 HASTINGS CONST. L.Q. 449 (2008); William Pollack, Note, *Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J.L. REFORM 221, 224-31 (2008). *See also supra* note 28.

61. The statute provides in pertinent part:

> Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that . . .
>
> (A) the electronic surveillance is solely directed at . . . (i)

also limited the application of the judicial authorization provisions of the statute.[62] Consistent with the technology of the period and the model provided by Title III, the law generally covered the acquisition of the contents of conversations when they involved United States persons, international communications with one end in the United States, or where the act of acquisition took place in the United States.[63] This made the law partially extra-territorial in effect,

---

> the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, . . .or (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power . . .
>
> (B) 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
>
> (C) [adequate minimization procedures are followed].

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(a)(1)(A)-(C), 92 Stat. 1783, 1786-87 (codified at 50 U.S.C. § 1802(a)(1)(A)-(C) (2006)). The section also includes requirements that the Justice Department report to the Chief Justice and pertinent House and Senate committees. *See id.* § 102(a)(1)-(3), 92 Stat. at 1786-87.

62. *Id.* § 101(f)(1)-(3), 92 Stat. at 1785 (codified at 50 U.S.C. § 1801(f)(1)-(3) (2006)).

63. The statute defines the term "electronic surveillance" as:

> (1) the acquisition by an electronic . . . device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic . . . device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . .
>
> (3) the intentional acquisition by an electronic . . . device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States . . . .

Id.

a fact noted in the Senate Report.[64] The definition of "foreign power" begins by tracking conventional usage to include foreign governments, factions, or foreign-based political organizations, but also includes international terrorism, defined as violent or otherwise dangerous actions that are both violations of criminal law and intended to intimidate governments or civilians.[65] Another central definition concerns "foreign intelligence information," which is defined in two respects. The information must relate to the nation's ability to protect itself from attack, sabotage, international terrorism or clandestine intelligence by foreign entities.[66] Alternatively, and far more generally, if a foreign power is involved, the information must relate to national defense or security or the conduct of foreign

---

64. *See* S. REP. NO. 95-604 (pt. I) at 40 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3942.

65. The statute includes as a definition of "foreign power," "a group engaged in international terrorism or activities in preparation therefor." Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(a)(4), 92 Stat. 1783, 1783 (codified at 50 U.S.C. § 1801(a)(4) (2006)). The statute also defines "international terrorism" as activities that:

> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
>
> (2) appear to be intended . . . (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and
>
> (3) occur totally outside the United States, or transcend national boundaries . . . .

Id. § 101(c)(1)-(3), 92 Stat. at 1784 (codified at 50 U.S.C. § 1801(c)(1)-(3) (2006)).

66. *Id.* § 101(e)(1), 92 Stat. at 1784 (codified at 50 U.S.C. § 1801(e)(1) (2006)). The statute states that "foreign intelligence information" includes:

> (1) information that relates to, and if concerning a United States person is necessary 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 (C) clandestine intelligence activities by an intelligence service or network of a foreign power . . .

Id.

affairs.[67] In both aspects, if the information concerns a United States person, then the information must be "necessary" to the ability to protect national defense, security, or foreign affairs.[68] The emphasis on protection for U.S. citizens and resident aliens from unjustified intrusion is a recurring theme in the statute and its legislative history.[69]

With respect to electronic surveillance of covered individuals for intelligence purposes, the law requires judicial permission somewhat analogous to the electronic surveillance warrants governed by Title III for traditional criminal activity.

The first of two key provisions regulating use of electronic surveillance with court involvement was included in Section 104 of FISA.[70] This provision includes numerous requirements for applications for court orders approving electronic surveillance. The central requirements are that the application include the facts supporting the conclusion that the target of the electronic surveillance is "a foreign agent or an agent of a foreign power" and that the facilities subject to the surveillance are used by a foreign power,[71] as well as "a detailed description of the nature of the information sought"[72] and a series of certifications by senior executive officials.[73] These certifications relate to the conclusion that the

67. *Id.* § 101(e)(2), 92 Stat. at 1785 (codified at 50 U.S.C. § 1801(e)(2) (2006)) (stating that foreign intelligence information also includes: "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 security of the United States; or (B) the conduct of the foreign affairs of the United States").

68. *See id.* § 101(e)(1)-(2), 92 Stat. at 1784-85 (codified at 50 U.S.C. § 1801(e)(1)-(2) (2006)) (each using the word "necessary").

69. *See, e.g.*, *id.* § 101(b), (e), (f), (h), 92 Stat. at 1783-86 (codified at 50 U.S.C. § 1801(b), (e), (f), (n) (2006)) (definitions dependent on whether person in question is a U.S. person). *See also* S. REP. NO. 95-604 (pt. I) at 40 (discussing the definition of "United States person" and noting controversies about the limited protections accorded to other persons).

70. *See id.* § 104, 92 Stat. at 1788-90 (codified as amended at 50 U.S.C. § 1804 (2006)).

71. *Id.* § 104(a)(4), 92 Stat. at 1788-89 (current version at 50 U.S.C. § 1804(a)(3) (2006)).

72. *Id.* § 104(a)(6), 92 Stat. at 1789 (current version at 50 U.S.C. § 1804(a)(5) (2006)). The current version of the statute no longer requires that the description be "detailed."

73. *Id.* § 104(a)(7), 92 Stat. at 1789 (current version at 50 U.S.C. § 1804(a)(6) (2006)). Again, the "foreign power" category now includes participants in international terrorism.

information is "foreign intelligence information,"[74] describing the appropriate statutory category,[75] and the basis for the certifications.[76] In the initial version of FISA, a required certification was that "the purpose of the surveillance" was to obtain foreign intelligence information.[77] In the USA-PATRIOT Act, Congress amended this required certification to require that "a significant purpose of the surveillance" be to obtain foreign intelligence information.[78] This subtle language distinction belies the substantial political and legal controversy concerning the purpose distinction between criminal investigation and foreign intelligence.

The second key provision regulating use of electronic surveillance with court involvement was Section 105 of FISA, or the "Issuance of order" provision.[79] This provision requires that the judge[80] make a series of findings concerning: proper authorization of the application within the Department of Justice,[81] probable cause,[82] minimization,[83] and compliance with all certification requirements.[84] The probable cause

74. *Id.* § 104(a)(7)(A), 92 Stat. 1789 (current version at 50 U.S.C. § 1804(a)(6)(A) (2006)).

75. *Id.* § 104(a)(7)(D), 92 Stat. 1789 (current version at 50 U.S.C. § 1804(a)(6)(D) (2006)).

76. *Id.* § 104(a)(7)(E), 92 Stat. at 1789 (current version at 50 U.S.C. § 1804(a)(6)(E) (2006)).

77. *Id.* § 104(a)(7)(B), 92 Stat. at 1789 (current version at 50 U.S.C. § 1804(a)(6)(B) (2006)).

78. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 218, 115 Stat. 272, 291, *amending* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B).

79. Foreign Intelligence Surveillance Act of 1978, § 105, 92 Stat. at 1790 (codified as amended at 50 U.S.C. § 1805 (2006)).

80. The judges referred to are members of a special court, known as the Foreign Intelligence Surveillance Court, which is made up of a select group of federal district court judges. *Id.* § 103(a), 92 Stat. at 1788 (codified as amended at 50 U.S.C. § 1803(a) (2006)). FISA also provides for a second court, comprised of three federal district or appellate judges, which reviews the denial of FISA applications. *Id.* § 103(b), 92 Stat. at 1788 (codified as amended at 50 U.S.C. § 1803(b) (2006)).

81. *Id.* § 105(a)(1)-(2), 92 Stat. at 1790 (codified as amended at 50 U.S.C. § 1805(a)(1) (2006)).

82. *Id.* § 105(a)(3), 92 Stat. at 1790 (current version at 50 U.S.C. § 1805(a)(2) (2006)).

83. *Id.* § 105(a)(4), 92 Stat. at 1790 (current version at 50 U.S.C. § 1805(a)(3) (2006)).

84. *Id.* § 105(a)(5), 92 Stat. at 1790 (current version at 50 U.S.C. §

requirement differs from that usually required for Fourth Amendment searches or seizures, including electronic surveillance. The issuing judge must determine, based on the application, that there is probable cause that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . [and that the telephone or location] is being used, or is about to be used, by a foreign power or an agent."[85] Other provisions of Section 105 concern more technical and formal requirements, including specifications in the judicial order such as periods of authorized use,[86] retention and use requirements,[87] emergency authorizations,[88] testing of equipment,[89] and liability issues.[90] The limitation of this probable cause requirement is important. In contrast to probable cause requirements in criminal investigations, there is no requirement that the judge find probable cause that the electronic surveillance will actually provide any foreign intelligence. Rather, the requirement is simply a probable cause finding that the target is a foreign power or agent. The connection between the nature of the target (the judicial finding) to the information important to national security is entirely contained in the certification requirements of Section 104. As noted above, a senior administration official must certify "that the certifying official deems the information sought to be foreign intelligence information . . . and that a significant purpose of the surveillance is to obtain foreign

1805(4) (2006)).

85. *Id.* § 105(a)(3)(A)-(B), 92 Stat. at 1790 (current version at 50 U.S.C. § 1805(a)(2)(A)-(B) (2006)). The omitted language within the quote is a proviso that prohibits concluding that a United States person is a foreign power or agent "solely upon the basis of" protected First Amendment activities. *Id.* § 105(a)(3)(A), 92 Stat. at 1790 (current version at 50 U.S.C. § 1805(a)(2)(A) (2006)).

86. *Id.* § 105(d), 92 Stat. at 1791 (codified as amended at 50 U.S.C. § 1805(d) (2006)).

87. *Id.* § 105(g), 92 Stat. at 1793 (codified at 50 U.S.C. § 1805(g) (2006)).

88. *Id.* § 105(e), 92 Stat. at 1791-92 (codified as amended at 50 U.S.C. § 1805(e) (2006)).

89. *Id.* § 105(f)(1), 92 Stat. at 1792 (codified at 50 U.S.C. § 1805(f)(1) (2006)).

90. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 225, 115 Stat. 272, 295-96 (current version at 50 U.S.C. § 1805(h) (2006)).

intelligence information."[91] Thus, the required connection to suspicious behavior is entirely based on the government's purpose.

3. What Was Not Subject to FISA

The gaps in FISA are significant. As enacted, the law governed only electronic surveillance of communications with a clear connection to the United States. This was consistent with executive branch policy throughout the last thirty years, policy that holds that *international* use of most investigative techniques, including electronic surveillance, is exempt from constitutional regulation and should remain exempt from congressional oversight.[92] Thus, FISA elaborated on the categories recognized in *Keith*. Some international intelligence operations came under this regulatory scheme,[93] while others apparently remained subject only to executive supervision.

91. 50 U.S.C. § 1804(a)(6)(A)-(B) (2006). *See also* 50 U.S.C. § 1823(a)(6)(B).

92. This fit into *Keith*'s rationale, which held that domestic electronic surveillance was not permitted by Congress in the 1968 law, but which was subject to constitutional requirements akin, if not identical, to those attending criminal law electronic surveillance. The Bush administration also took the view that any attempt by Congress to regulate international use of investigative techniques, at least in the context of the war on terrorism, would be an unconstitutional infringement on the Commander-in-Chief power. *See* Letter from Alberto R. Gonzales, Attorney General, to Majority Leader, U.S. Senate (Jan. 19, 2006), http://www.justice.gov/olc/2006/nsa-white-paper.pdf. *See also* John Cary Sims, *How the Bush Administration's Warrantless Surveillance Program Took the Constitution on an Illegal, Unnecessary, and Unrepentant Joyride*, 12 UCLA J. INT'L L. & FOREIGN AFF. 163 (2007).

93. More recently, supporters of broad executive power have argued that any congressional regulation of intelligence surveillance is unconstitutional. *See* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* http://epic.org/privacy/terrorism/fisa/doj11906wp.pdf. This is fine as a matter of governmental theory. There is not a lot of law to support this view, however, other than *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304 (1936). That case includes language that on its face supports robust executive powers in the international sphere. *Curtiss-Wright*, 299 U.S. at 320. The underlying premise of *Curtiss-Wright*, however, is that the President is supreme with respect to carrying out international aspects of U.S. law, such as conducting relations with foreign nations—not with respect to making United States international law. The decision itself upheld congressional action authorizing executive action, much as FISA does. *Id.* at 312-22.

Domestic intelligence investigation, such as that involved in *Keith,* presumably remained subject to Title III and would be permitted only upon meeting the demanding standards of that statute.

Over the years, additional gaps in FISA have been discovered, and some have been filled. For example, new technologies, such as email communications and cell-phones, have necessitated statutory amendments to expand investigative powers.[94] This was a major issue in the early years of the War on Terrorism, when the Bush Administration credibly argued that FISA was outdated.[95]

The most notable gap, however, would seem to be that FISA does not cover *criminal* investigations, even those that might involve foreign powers or international terrorists. This was not an oversight. Title III still applies to criminal investigations and, in fact, specifically provides for court-ordered electronic surveillance under traditional standards for many federal crimes generally committed by foreign agents or terrorists.[96] Most telling is the fact that Title III was amended after FISA was enacted to include some of these crimes, including crimes that, by definition, involve international terrorism.[97] The difference between FISA and Title III is that

---

94. *See, e.g.*, United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 206, 115 Stat. 272, 282 (codified as amending 50 U.S.C. § 1805(c)(2)(B) (2006)) (granting roving surveillance authority to FISA intercept orders to allow agents to follow a target's communications without additional court action where the target changes communication services). *See also* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225 (2008) (discussing the need to modernize FISA); Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 L. LIBR. J. 601 (2002).

95. *See, e.g.*, *Concerning the Foreign Intelligence Surveillance Act: Hearing on S. 2248 Before the S. Comm. On the Judiciary*, 110th Cong. (2007) (statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice), *available at* http://www.justice.gov/archive/ll/docs/final-wainstein-sjc-testimony-103007.pdf; Michael B. Mukasey, Op-Ed., *A FISA Fix*, L.A. TIMES, Dec. 12, 2007, at 31; Eric Lichtblau, *Deal is Struck to Overhaul Wiretap Law*, N.Y. TIMES, June 20, 2008, at A1.

96. *See* 18 U.S.C. § 2516(1) (2006) (providing for use of Title III electronic surveillance for crimes including espionage, sabotage, violence at international airports, and terrorist attacks).

97. *See id.* § 2516(q) (providing that Title III orders are permitted for

FISA applies to investigations that seek foreign intelligence, while Title III applies to those that are essentially attempts to collect evidence for criminal prosecution. This is the only reading consistent with the case law of the period, *Keith* and *Truong*.

B. *FISA Over the Years*

1. The Judicial Response

Although *Truong* is heavily cited, as discussed above, it addressed pre-FISA electronic surveillance, and is therefore most applicable to claims of inherent presidential power. Several other circuit court decisions did, however, address the meaning and application of FISA after its enactment. One such case is *United States v. Duggan*, which reviewed a conviction based in part on FISA electronic surveillance of Provisional Irish Republican Army members who came to the United States to obtain weapons and other items for use in paramilitary actions in Northern Ireland.[98] That court considered several constitutional challenges to FISA.[99] It noted that prior to FISA, courts were generally supportive of a presidential power to conduct warrantless electronic surveillance in the foreign intelligence sphere.[100] It also accurately described *Keith* as limited to domestic surveillance and signaling approval of a flexible application of the Fourth Amendment in the intelligence sphere.[101] The court then reasoned that FISA was Congress' attempt to take up the Supreme Court's suggestion in *Keith* concerning flexible application and to resolve Fourth Amendment questions in the intelligence sphere through the complex machinery of the

---

crimes related to the use of chemical weapons and various additional crimes relating to terrorism).

98. United States v. Duggan, 743 F.2d 59, 65-67 (2d Cir. 1984).

99. *See, e.g.*, *id.* at 71-75 (presenting arguments that the law was so broad and vague as to deny due process, that it violated the Fourth Amendment by not requiring probable cause of criminal conduct, and that it violated Equal Protection by providing less protection to lawful non-resident aliens than to citizens and resident aliens; the court refused to bite at any of these arguments).

100. *Id.* at 72.

101. *Id.* at 72-73.

statute.[102] Using constitutional interest-balancing, the court concluded that FISA's procedures reflected a reasonable balance of rights and intelligence needs.[103] Thus, the court upheld the law and acknowledged that there was no probable cause requirement if the surveillance "will in fact lead to the gathering of foreign intelligence information."[104] The court also upheld the *in camera* review of the affidavits and certifications to determine compliance with FISA and the Fourth Amendment.[105]

The *Duggan* court briefly referred to the "other purposes" issue, concluding that courts should generally accept the government's certifications on the issue of purpose.[106] The court understood that there is a logical connection between intelligence information and evidence of criminal behavior, and seemed to see this as a reason to allow both the surveillance for intelligible purposes, along with the use of its resulting evidence in criminal prosecutions.[107] The court did recognize that there would be room for challenges, however, concluding that general Fourth Amendment doctrine concerning false assertions in search warrant paperwork would be applicable.[108] Accordingly, it indicated that a false assertion that the electronic surveillance was for foreign intelligence would be a violation of FISA.[109] It would necessarily also be a violation of the Fourth Amendment, as the combined effect of *Keith* and FISA meant that domestic electronic surveillance would be

---

102. *Id.* at 73.

103. *Id.* at 72-73. Of particular note, the court recognized that the probable cause findings relate to the target's status and use of the telephone or other instrument of electronic surveillance. *Id.*

104. *Id.* at 73.

105. *Id.* at 78.

106. *Id.* at 77.

107. "Finally, we 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 recognized in 1806(b), as evidence in a criminal trial." *Id.* at 78.

108. *Id.* at 77. The court referred to *Franks v. Delaware* and by analogy required a person challenging a FISA purpose certification "to make 'a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application." *Id.* (quoting Franks v. Delaware, 438 U.S. 154, 155-56 (1978)).

109. *Id.*

outside the parameters of both FISA and Title III, and therefore unconstitutional.[110]

2. The Wall

Based in part on *Truong* and other cases even more explicit about the purpose limitation of FISA, the government began to carefully limit access by criminal investigators and prosecutors to intelligence obtained in FISA electronic surveillance, and vice versa. The rationale of this "wall," as it became known, was to protect both types of government investigations. Information obtained under FISA would not be shared with criminal investigators in many instances in order to protect criminal cases from being "tainted," should it later be determined that its use was inappropriate. The purpose of the wall in the other direction is less obvious.[111]

David Kris, who served in a senior capacity at the Justice Department in the early years of the Bush Administration–the period in which the wall was largely dismantled—argues that the wall was never required by law.[112] He traces the path by which all three branches of government, including both Republican and Democratic presidential administrations,

110. Other courts of the pre-2001 period tended to follow *Truong* and accept the "primary purpose" theory. *See, e.g.*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Rahman, 861 F. Supp. 247, 251 (S.D.N.Y. 1994) (decided by future Attorney General Michael B. Mukasey). *But cf.* United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988) (addressing but not deciding the issue).

111. FISA would not apply to those investigations, but arguments could be built on the limitations on use of Title III electronic surveillance and grand jury evidence to prevent consideration in intelligence, as opposed to law enforcement, matters.

112. Kris served as Associate Deputy Attorney General during the Bush Administration, and now serves as Assistant Attorney General for National Security. *See* U.S. Dep't of Justice, National Security Division: Mission and Function, www.justice.gov/nsd/bio.htm (last visited Jan. 29, 2010). He has written a detailed study of the wall. *See* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006). Kris is no supporter of the wall, but his description of its history is more measured than that of most articles by people on either side of such hot-button topics. Kris was a litigator in the case that supposedly ended the wall, *see In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002), and he describes himself as one of its principal authors, Kris, *supra*, at 487 n.* (unnumbered footnote), but his view on the underlying flaw in the wall was not adopted by that court.

created largely separate intelligence and law enforcement tracks.[113] The most notable point in this history was in 1995, when the Department of Justice's Office of Legal Counsel issued a memorandum concluding that the wall was central to convincing courts that a foreign intelligence electronic surveillance satisfied the primary purpose test.[114] This memorandum was soon followed by a March memorandum from Deputy Attorney General Jamie S. Gorelick,[115] as well as by a July memorandum from Attorney General Janet Reno[116] on policies and procedures for coordinating law enforcement and foreign intelligence investigations. In general, these documents accepted the primary purpose requirement, and therefore directed that foreign intelligence electronic surveillance be limited to matters in which obtaining such intelligence was the primary purpose.[117] The documents then went beyond the apparent legal requirements by limiting disclosure and minimizing reliance on joint investigative teams.[118] Kris argues that, while the Department of Justice policies encouraged coordination in some respects, their practical effects were to limit coordination.[119] Early in the Bush Administration, several policy changes served to enhance coordination, but most aspects of the wall still remained in place in September 2001.[120]

The existence of the wall and the impact of limiting information concerning terrorist activities became a major controversy after the September 11 attacks. The Department of Justice issued new guidelines permitting much more contact

---

113. Kris, *supra* note 112, at 499-506.

114. *Id.* at 499 & n.69 (citing Memorandum from Walter Dellinger, Assistant Attorney General for the Office of the Legal Counsel, to Michael Vatis, Deputy Director, Executive Office for National Security (Feb. 14, 1995) (on file with Kris)).

115. *See id.* at 501 & n.79 (citing Memorandum from Jaime S. Gorelick, Deputy Attorney General, to Mary Jo White, U.S. Attorney, Southern District of New York et al. (March 1995), http://www.justice.gov/ag/testimony/2004/1995_gorelick_memo.pdf).

116. *See id.* at 504 & n.99 (citing Memorandum from Janet Reno, Attorney General, to Assistant Attorney General of the Criminal Division et al. (July 19, 1995), http://www.fas.org/irp/agency/doj/fisa/1995procs.html).

117. *Id.* at 501-06.

118. *Id.* at 503.

119. *Id.*

120. *Id.* at 507-08.

between investigative and intelligence operatives.[121] Attorney General Ashcroft also chose to raise the issue during his testimony before the September 11 Commission, as he accused Gorelick, by then a member of the Commission, of responsibility for intelligence lapses leading to the attacks as a result of her role in establishing the wall.[122]

3. The 1995 Authorization of Surreptitious Searches

In 1995, Congress amended FISA to permit physical searches within the United States under standards and procedures similar to those applicable to electronic surveillance.[123] Thus, intelligence officers could conduct actual entries into private buildings, including homes, without meeting the probable cause standard generally applicable to criminal searches. Such searches could occur over a period of up to one year, even without judicial approval, if the premises were not those of a covered "U.S. person."[124] The most noteworthy aspect of such searches is not the absence of the traditional probable cause requirement, or the fairly limited judicial role.[125] Instead, it is the fact that the searches are by

121. *See id.* at 507-11.

122. *See* ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE 269-73 (2009). The book by Thomas Kean and Lee Hamilton, Chairs of the 9/11 Commission, addresses some of the Commission's conflicts with Ashcroft on various issues. *See* THOMAS H. KEAN & LEE H. HAMILTON, WITHOUT PRECEDENT: THE INSIDE STORY OF THE 9/11 COMMISSION (2006). The Chairs found Ashcroft to be very hard to deal with, perhaps because of leaks criticizing him that came from inside the Commission. *Id.* at 194. He stage-managed his testimony very dramatically, as evidenced by his refusal to provide written copies of his formal statement before reading it on national television. *Id.* While all witnesses defended their own turf and criticized others to some degree, Kean and Hamilton characterize Ashcroft as the most defensive and antagonistic witness, and argue that he attacked Gorelick far beyond what the record could support. *Id.* at 194-96. They argue that he changed facts to manipulate public reaction, and note that even the Republicans on the Commission would not accept his assertions. *Id.* at 196. They also claim that President Bush disapproved of this behavior, indicated that it would stop, and largely ignored Ashcroft after his confrontation with the Commission. *Id.* at 208-10.

123. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443-3453 (codified as amended at 50 U.S.C. § 1822-29 (2006)).

124. 50 U.S.C. § 1822(a)(1) (2006).

125. The statute provides for the contents of the application to the FISA

their nature surreptitious. The multiple entries and year-long authorization periods established by the statute necessarily mean that entries will be secret and unreported to the owner or occupant, conceivably forever. The statute provides for notice only after the end of the national security interest.[126]

These so-called "sneak and peek" searches are not limited to intelligence matters. They have been permitted since the 1979 Supreme Court decision of *Dalia v. United States*, which authorized surreptitious physical entries in connection with installation of electronic surveillance equipment.[127] Still, outside of the foreign intelligence setting, such searches are carefully limited in several respects. Traditional probable cause is a requirement, as is notice, although it comes after a delay.[128]

---

court, including, as amended in 2001, the "significant purpose" requirement and the findings required in the order authorizing the search. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 218, 115 Stat. 272, 291, *amending* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (current version at 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B)).

126. 50 U.S.C. § 1825(b) (2006). This portion of FISA contains many other detailed provisions on physical searches, including notifications when U.S. persons are involved, suppression standards, and *in camera* review. *Id.* § 1825.

127. Dalia v. United States, 441 U.S. 238 (1979). The Court interpreted Title III as authorizing surreptitious entry for the purpose of installing and maintaining the court-ordered listening device, noting that "[t]he plain effect of the detailed restrictions of § 2518 is to guarantee that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed." *Id.* at 250.

128. See Section 3101a of Title 18 of the *United States Code*, which was enacted as part of the USA-PATRIOT Act:

> Delay—With respect to the issuance of any warrant or court order . . . to search for and seize any property or material that constitutes evidence of a criminal offense . . . any notice required . . . may be delayed if . . . the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result . . . [;] the warrant prohibits the seizure of any tangible property, any wire or electronic communication . . . , except where the court finds reasonable necessity for the seizure; and . . . the warrant provides for the giving of such notice within a reasonable period not to exceed 30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

C. *The USA-PATRIOT Act Amendment*

1. The Statutory Change

As noted above, the USA-PATRIOT Act included a provision that was intended to break down the wall. According to Assistant Attorney General Kris, after the September 11 attacks, the Department of Justice sent to Congress an amendment to FISA that would allow foreign intelligence electronic surveillance when "*a* purpose" rather than "*the* purpose" of the electronic surveillance or surreptitious search was to obtain foreign intelligence information.[129] Congress later changed the standard, opting for "a significant purpose," which was far more limited than the Department had wanted, but significantly more generous than the previous statutory requirement that "the" purpose be to obtain foreign intelligence information.[130] This would seem likely to change the test that has been followed in most courts, which requires that intelligence be the primary purpose of the investigation.

---

18 U.S.C. § 3101a(b)(1)-(3) (2006). The "adverse result" is defined in Section 2705 of Title 18 and includes: "(1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial." § 2705(a)(2). These reasons are intrinsically different from those applicable to surreptitious FISA searches, which are, as they should be, focused on gaining information about foreign intelligence.

129. Kris, *supra* note 112, at 508 (emphasis added) (discussing the USA-PATRIOT Act's amendments to 18 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (now codified at 18 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (2006)). By this time, of course, the change would also allow greater use of physical searches. *See* discussion *supra* Part I(B)(3).

130. On changes to FISA and other statutes governing investigative powers during this period, see ANNA C. HENNING & EDWARD C. LIU, CONG. RESEARCH SERV., AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) SET TO EXPIRE IN 2009 (2009), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA509762&Location=U2&doc=GetTRDoc.pdf; GINA MARIE STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., PRIVACY: AN ABBREVIATED OUTLINE OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING (2009), *available at* http://www.fas.org/sgp/crs/intel/98-326.pdf; Robert Bloom & William J. Dunn, *The Congressional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147 (2006); Burton, *supra* note 60; Pikowsky, *supra* note 94.

This subtle distinction was potentially important. Under the previous test, the main purpose had to be intelligence gathering—the government had to be seeking information to help in its future responses to international developments or terrorism. Collection of evidence for criminal prosecution was welcome and could be anticipated if the targets revealed their involvement in actions punishable under U.S. criminal law, but obtaining such evidence could not be the primary objective. The wall, of course, was one way of indicating adherence to this principle. Agents from the intelligence side dominated the planning and execution of FISA surveillance, and information was shared with criminal investigators only where it could be established that such action was subsidiary to a dominant intelligence purpose.[131] Under the revised version, apparently the only requirement was that the agents establish that seeking foreign intelligence was a non-trivial part of the enterprise.[132] This would seem self-evident in most cases. As such, the wall was anachronistic, at least as far as FISA was concerned. The Department responded by dismantling the wall internally to some degree, and then by seeking to have the FISC modify requirements in FISA orders to reflect the greater power of the government to share information obtained in electronic surveillance.[133]

2. Judicial Responses to the 2001 Amendment

The battle over the 2001 amendment began in earnest in

131. The wall operated in slightly different ways during different periods. *See* Kris, *supra* note 112, at 499-505 ("History of the FISA Wall" through USA-PATRIOT Act amendment to FISA).

132. Kris addresses several ramifications of the wall, addressing both civil liberties and security concerns. Kris, *supra* note 112, at 518-21. The wall is largely irrelevant to who is subject to surveillance and what information is sought or intercepted. *Id.* at 519. FISA targets usually commit crimes relevant to espionage or terror, but could also commit unrelated crimes. Kris suggests non-international or non-terrorism crimes, such as child pornography or theft, both of which often involve computers and communication systems. *Id.* at 519-20. A prosecutor might want to scrutinize a target's email accounts for both types of offenses. There can be legitimate national security reasons to pursue unrelated offenses by national security targets, if only because additional criminal liability might result in a cooperative witness rather than a silent defendant. *Id.* at 520-23.

133. This is described, from an insider's perspective, in Kris, *supra* note 112, at 510-11.

2002 when the FISC issued a general order restricting the Department of Justice's use of FISA to investigations not primarily intended for criminal prosecution.[134] The conflict arose in the context of motions by the Department of Justice to vacate minimization and wall procedures in matters then before the FISC. The FISC approved some of the government's requested changes but denied others. Rather than permit the fairly unregulated joint operation of intelligence and law enforcement investigations requested by the Department of Justice, the court ruled that the following language should be included in FISA orders:

> The FBI, the Criminal Division, and [the Office of Intelligence Policy and Review] may consult with each other to coordinate their efforts to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism or clandestine intelligence activities by foreign powers or their agents. Such consultations and coordination may address, among other things, exchanging information already acquired . . . and overall strategy of both investigations in order to ensure that the overlapping intelligence and criminal interests of the United States are both achieved. . . . [[T]he Office of Intelligence Policy and Review] shall be invited to all such consultations, and if they are unable to attend, [they] shall be apprised of the substance of the consultations forthwith in writing so that the Court may be notified at the earliest opportunity.
>
> Notwithstanding the foregoing, law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division

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

> shall ensure that law enforcement officials do not direct or control the use of FISA procedures to enhance criminal prosecution . . . .[135]

The key language, of course, was the ban on law enforcement officials taking a supervisory role, which might suggest that criminal enforcement rather than intelligence collection purposes were dominant. In effect, the court partially reversed the Department's decision to lower the wall, but acted through the minimization requirements of FISA, rather than through the "intelligence purpose" requirement.[136]

These provisions were included in two electronic surveillance orders issued later that year, and the Department of Justice appealed to the Foreign Intelligence Surveillance Court of Review ("FISCR").[137] That court overturned the FISC's restrictions in a decision that took the lower court to task. First, the FISCR reached out to decide that the use of the wall was inappropriate, even under the original text of FISA that was enacted in 1978.[138] This was unnecessary because the court's interpretation of the amended version of the statute would have itself resolved all issues pertinent to the dispute, and the Department of Justice had not even made this broader argument in the court below. Nevertheless, the FISCR addressed the history of surveillance authorizations under FISA and concluded that nothing in the original statute mandated the high wall imposed by the Department and, now, by the FISC.[139] The FISCR concluded that *Truong* was inapplicable to FISA cases and had been blindly followed, rather than intelligently applied, in the federal appellate cases that followed it by adopting the "primary purpose" test.[140]

The FISCR then addressed the status of joint "intelligence/criminal" investigations under the 2001 amendments to FISA. It concluded that the statutory revision

---

135. *Id.* at 625.

136. *See id.* at 616-20 (characterizing action as part of minimization requirements).

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

138. *Id.* at 722-28.

139. *Id.* at 723-25.

140. *Id.* at 725-28.

resolved any doubt on this issue.[141] This allowed the government to use FISA procedures in cases in which criminal prosecution was in fact the primary motivation of the investigation. The FISCR stated that "the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses."[142] The opinion concluded by reexamining these issues through the prism of the Fourth Amendment. Here the FISCR found the FISA process lawful as long as the government was in fact acting through its foreign intelligence powers.[143] That is, as long as the government was seeking information on foreign intelligence as defined in FISA, it could use the more lenient procedures permitted by FISA rather than the traditional requirements imposed in criminal investigations.[144]

The two courts therefore confronted similar, yet different, issues. The FISC looked to minimization, a statutory requirement that had not been changed from the original FISA provisions, and which required that electronic surveillance be conducted so as to minimize the intrusion on U.S. persons, largely by limiting disclosure and use of intercepted conversations (and evidence discovered in surreptitious searches).[145] Accordingly, the FISC limited the disclosure and

141. *Id.* at 728-38.

142. *Id.* at 735.

143. *Id.* at 736-37.

144. *Id.* at 745. Kris's argument, which was part of the government's argument to the FISCR, was that there was no dichotomy between law enforcement and foreign intelligence searches because the President has the constitutional authority to act to protect national security through law enforcement, and therefore, the less demanding FISA procedures apply to criminal investigations conducted in order to protect national security. Kris, *supra* note 112, at 519-23. The short answer to this point is that, just as the President and Congress have powers with respect to criminal prosecutions for offenses such as counterfeiting or piracy, their choice to use the criminal processes means that the constitutional (and other) laws relating to the criminal process are presumably applicable. In other words, a presidential decision to use the criminal law to achieve national objectives beyond law enforcement does not eliminate the Fourth Amendment's requirement of reasonable searches and seizures any more than it permits evading the First Amendment's rights of free speech or the Eighth Amendment's prohibition of cruel and unusual punishment.

145. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 615 (FISA Ct. 2002).

use of those conversations for non-foreign intelligence purposes.[146] On appeal, the FISCR, however, largely accepted the Department of Justice's argument that the modification of FISA by the USA-PATRIOT Act eliminated any need to separate intelligence investigations from dual purpose intelligence/criminal investigations.[147]

The few cases that have addressed this issue indicate a trend to accept the FISCR analysis of *In re Sealed Case*. The Seventh Circuit adopted this reasoning in *United States v. Ning Wen*.[148] Three 2008 federal district court decisions also upheld the view that the USA-PATRIOT Act amendment was constitutional and that the law now permits the use of FISA to collect evidence for criminal prosecutions.[149] As of August 2009, the only noteworthy decision to the contrary is a district court decision involving Brandon Mayfield, the Oregon attorney mentioned in this article's Introduction, who was wrongly accused of involvement in the 2004 Madrid train bombing.[150] That decision held that the 2001 amendment was unconstitutional on Fourth Amendment grounds, essentially finding that the authorization to engage in intrusive searches of criminal suspects without probable cause of criminal activity rendered the law unconstitutional even where there is a factual connection to an intelligence purpose.[151]

There is little reason to doubt that the FISCR's view will prevail, at least in the short run. The primary purpose test had a long pedigree, but the USA-PATRIOT Act constituted a

---

146. *Id.* at 617.

147. *In re* Sealed Case, 310 F.3d at 722, 732. It is fair to conclude that neither court had it quite right. While minimization is required by statute as well as, arguably, the Fourth Amendment—for at least some FISA surveillance—the FISC's broad generic ruling did not respond to the real issue. The FISCR, on the other hand, had the right issue—law enforcement purposes for FISA surveillance—but overlooked the constitutional line drawn by the Supreme Court between law enforcement and special needs searches. *See generally* discussion *infra* Part III.

148. United States v. Ning Wen, 477 F.3d 896 (7th Cir. 2007).

149. One, of course, is United States v. Abu-Jihaad, 531 F. Supp. 2d 299 (D. Conn. 2008). *See also* United States v. Warsame, 547 F. Supp. 2d 982 (D. Minn. 2008); United States v. Mubayyid, 521 F. Supp. 2d 125 (D. Mass. 2007).

150. Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated*, 588 F.3d 1252 (9th Cir. 2009).

151. *Id.* at 1042.

congressional willingness to loosen the requirement. On top of that, until 2002, federal courts had no FISCR precedent to draw upon, and *Truong* and other cases dealing with the original FISA therefore became the basic decisions in the field. With the FISCR ruling, however, the precedent now comes from a court with specific delegated authority to decide FISA issues,[152] and it is unlikely that the Oregon precedent in *Mayfield* will convince many other lower courts. Perhaps more significantly, the FISCR decision is from a court with nationwide jurisdiction and which provides the primary appellate judicial supervision of the FISA process. As such, decisions to the contrary, such as *Mayfield*, may seem to be trivial outliers to other courts. FISA judges are themselves bound to follow the precedent of *In re Sealed Case*, and government agents involved in FISA investigations will have every reason to follow the "law" of the FISCR.[153] For example, one court that took other constitutional and statutory challenges to government actions in an intelligence investigation very seriously treated this challenge to the use of FISA evidence as insignificant.[154] As shown below, while this is arguably consistent with traditional Fourth Amendment law,

152. There is somewhat of a practical anomaly here, however, as the seven FISA judges who agreed to the ruling in *In re All Matters* had probably much more experience under the law than the three judges on the FISCR who reversed that ruling. *In re Sealed Case* was the first appeal considered by the FISCR. 310 F.3d at 719. The seven judges of the FISC all concurred in *All Matters*. 218 F. Supp. 2d 611, 625 (FISA Ct. 2002). During the seven years preceding the 2002 litigation, FISC judges had considered—and approved—over 5000 applications for FISA orders. *See* Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2007, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Feb. 14, 2010).

153. There is also reason to believe that the government could more readily evade facing courts that may lean toward *Mayfield* through venue selection. In contrast to criminal investigations under Title III, in which the circuit law that narrows government authority in a particular area must be followed within the districts that make up the circuit, here the FISCR would seem to set the law under which surveillance is conducted. At most, adverse circuit law would preclude criminal prosecutions based on evidence obtained during the electronic surveillance within those jurisdictions.

154. In *Turkmen v. Ashcroft*, the court simply drew an analogy to routine criminal searches and concluded that there is no credible objection to using in a criminal setting evidence obtained through national security electronic surveillance. Turkmen v. Ashcroft, No. 02CV2307(JG), 2006 WL 1662663, at *1 (E.D.N.Y. June 14, 2006), *aff'd, rev'd on other grounds per curiam*, 589 F.3d 542 (2d Cir. 2009).

there are credible arguments to the contrary, and the courts should not blindly follow *In re Sealed Case* any more than they should have blindly followed *Truong*.

II. Foreign Intelligence Searches in the Fourth Amendment Universe

A. *Special Needs*

This structure established by FISA, to allow electronic surveillance where foreign intelligence is a significant purpose of the action, is arguably consistent with the prevailing law concerning Fourth Amendment searches and seizures. In a series of decisions over the last thirty years, the Supreme Court has approved searches and seizures, and later use of resulting evidence in court, where the government had acted for a legitimate, non-law-enforcement reason, even where the government did not meet traditional Fourth Amendment requirements.[155] This is the "special needs" exception to the warrant and probable cause requirements. If the action is "reasonable" under the Fourth Amendment, then the intrusion is lawful.[156] Because the action is lawful under the Fourth Amendment, there is no reason to exclude the resulting evidence in criminal trials.

There are at least two legs to this principle in operation. One is that courts are reluctant to second guess law enforcement motives. If a government agent has a lawful basis to search, the courts will not invalidate the search or bar use of the seized evidence just because the officer took advantage of that basis to search, even though the officer hoped or anticipated finding evidence for a criminal prosecution. Another, sometimes related, principle is the Plain View Doctrine, in which the courts allow the seizure of evidence discovered under one rationale when there is some second reason that allows its seizure.[157] These notions arguably come

155. *See generally infra* notes 159-82 and accompanying text.

156. *See* Anthony C. Coveny, *When the Immovable Object Meets the Unstoppable Force: Search and Seizure in the Age of Terrorism*, 31 AM. J. TRIAL ADVOC. 329 (2007).

157. *See infra* notes 189-93 and accompanying text.

together in the Pretense Search Doctrine, in which the courts conclude that police officers may take advantage of reasonable suspicion or probable cause to stop a car for a vehicular violation while intending to look for evidence of more serious crimes.[158] While these doctrines were hotly disputed when first recognized, and while they do present significant questions about the nature of Fourth Amendment protections, they are unlikely to be reconsidered unless there is a sea change on the Supreme Court. Analyses of Fourth Amendment aspects of national security law must accordingly take them into account. To this end, the following section builds on "special needs" law and these principles to provide an argument for dual purpose foreign intelligence/law enforcement electronic surveillance under FISA.

The "special needs" doctrine was largely undeveloped when *Keith* was decided. The general principle developed in a series of cases in the late twentieth century, and is most closely associated with *New Jersey v. T.L.O.*[159] Over time the courts have established four controlling factors: 1) the "gravity of the public concerns" leading to the search or seizure, 2) the extent to which the search or seizure in fact advances those concerns, 3) the severity of the intrusion, and 4) the existence of a non-law enforcement purpose.[160] There are several different ways of organizing the resulting case law, but the most applicable to foreign intelligence searches separates those settings that involve what appear to be traditional searches and which are reasonably likely to result in evidence that can be used in criminal cases, from other cases that are more obviously civil in nature. The first quasi-criminal category can be distinguished from those that involve intrusions different in kind from law enforcement searches, such as drug tests,[161] or those that only

158. *See infra* notes 194-199 and accompanying text.

159. The case involved a search of a high school student's purse by a school assistant principal who had reason to believe she had been smoking in the women's restroom in violation of school rules. New Jersey v. T.L.O., 469 U.S. 325, 328 (1985).

160. *See* Illinois v. Lidster, 540 U.S. 419 (2004). In that case, police officers conducted a blockade near the scene of a fatal highway accident and handed out fliers in an attempt to locate witnesses to the incident. As a result of the blockade, Lidster was discovered to be driving under the influence of alcohol. *Id.* at 422.

161. *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989) (drug testing of employees in transportation industries); Nat'l

indirectly involve government agents examining private items or information.[162] By examining the four factors in the context of a quasi-traditional search such as electronic surveillance, the four factors largely devolve into a fairly raw balancing of two factors. In order to argue for the exception, the purpose must not be law enforcement, so factor (4) is a "yes/no" question that must be resolved prior to applying the rest of the test. The first two parts of the test, factors (1) and (2), seem complementary and together add up to an overall evaluation of the value of such searches to the government.[163] The severity of the intrusion, factor (3), is thus weighed against the value (both the abstract importance of the purpose and the degree aspects of parts (1) and (2)), in a manner typical of constitutional balancing tests.

Border searches provide a good example of "special needs" searches and reveal that they are not limited to new problems or new legal rules.[164] A more recent example is air security searches. The limitations on privacy in air travel began several decades ago with the rise of national security concerns, primarily the use of commercial aviation by hijackers to defect, or to otherwise engage in international terrorism.[165] Such

---

Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989) (drug testing of government employees involved in law enforcement).

162. This would seem to be the case with *T.L.O.* itself. The Fourth Amendment was involved in a school's policy because the school was public, but the underlying policy of keeping contraband off school property was not inherently a law enforcement or even governmental policy, as private schools would be expected to impose the same or similar rules.

163. This is reminiscent of the means/ends approach used in Due Process and Equal Protection—here, the overall purpose must be important and the intrusion must advance it to some unspecified degree. *See* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW ¶ 11.7 (8th ed. 2010) (identifying due process/fundamental rights standards of review); *id.* ¶ 14.3 (identifying equal protection standards of review).

164. The courts have confirmed that searches at the nation's borders are reasonable without warrants or probable cause due to the great national interest in protecting the nation from harmful persons or things entering or exiting the nation. *See* United States v. Flores-Montano, 541 U.S. 149, 152-53 (2004). While this power is an aspect of sovereignty and international law rather than law enforcement, the Fourth Amendment applies, but has very limited concern. Searches may include examination of the contents of vehicles, containers, personal property, and the like. *See, e.g.*, Chehade Refal v. Lazaro, 614 F. Supp. 2d 1103, 1112-15 (D. Nev. 2009) (collecting cases).

165. *See generally* James L. Buchwalter, Annotation, *Validity of Airport Security Measures*, 125 A.L.R. 5th 281, § 2a (2005). *See also* United States v. Bell, 464 F.2d 667 (2d Cir. 1972) (early reliance on hijacker profile); United

concerns led to security measures at odds with traditional Fourth Amendment protections. The primary use of evidence resulting from security searches, however, seems to be in enforcement of routine criminal laws. Such searches are not undertaken for criminal law enforcement purposes, but are at least similar in operation to law enforcement searches. Agents conducting air security searches look into private containers or on individuals themselves for weapons or other dangerous items. Contraband drugs and dangerous weapons, typical of the items discovered during such searches, are routinely used as evidence in criminal cases. Stated differently, a search of a suitcase at an airport security checkpoint does not differ much from a search of a suitcase during a criminal investigation except that the purpose is security rather than law enforcement.[166]

Air security searches are now commonplace, as anyone who has traveled by air in recent years can attest. They are also legally unimpeachable. Typical of cases upholding air security searches is *United States v. Edwards*, decided in 1974, a time at which such searches were far more limited than in the post-2001 period.[167] Edwards was an air passenger who had activated a magnetometer and became subject to a search of her carry-on baggage.[168] In a bag, wrapped in highly personal items, the inspector found glassine envelopes that contained heroin.[169] The majority engaged in a fairly simple interest-balancing analysis, and decided that the potential harm of air piracy was sufficiently grave to justify personal searches at airport gates to prevent passengers from taking

States v. Epperson, 454 F.2d 769 (4th Cir. 1972) (reliance on magnetometer to identify potential hijackers).

166. There are also serious privacy concerns about data mining of air passengers. *See, e.g.*, Stephen W. Dummer, Comment, *Secure Flight and Data Veillance, A New Type of Civil Liberties Erosion: Stripping Your Rights When You Don't Even Know It*, 75 MISS. L.J. 583 (2006).

167. United States v. Edwards, 498 F.2d 496 (2d Cir. 1974). *See also* United States v. Hartwell, 436 F.3d 174 (3d Cir. 2006) (modern decision upholding airport security searches); United States v. Aukai, 440 F.3d 1168 (9th Cir. 2006) (same); Buchwalter, *supra* note 165, §§ II(A)(4)-(7), (9)-(10) (collecting cases).

168. Today, of course, all air passengers are subject to searches of carry-ons and checked baggage, and at many airports, full body scans, somewhat akin to virtual strip searches, are used for many passengers.

169. *Edwards*, 498 F.2d at 499.

dangerous items on-board.[170] The judges used the balancing methodology then predominant to conclude that such intrusions are reasonable.[171] Judge Friendly's majority opinion did note a reservation that foreshadowed the "non-criminal purposes" requirement, that if "the Government is abusing its authority" by using air security searches as a general means of enforcing the criminal law, the search would be invalid and the evidence inadmissible.[172]

This exception is no longer limited to air security. The Second Circuit considered a New York City policy of conducting random, suspicionless container searches of persons entering the subway system.[173] The Court held that because the program was not a "general means of enforcing the criminal law," the validity of the search under the Fourth Amendment was measured under the far more lenient general balancing of costs and benefits.[174] Here, the public interest in preventing attacks on the subways is obvious and compelling. Given the then-even more recent international history of subway attacks, it is remarkable that there was any debate on the issue at all.[175] Cases with little connection to international terrorism reveal the extent to which the expanded notion of governmental security search powers has pervaded the law. This concern arose in *United States v. Va Lerie*, in which cocaine was discovered in a search of a garment bag removed from a bus luggage compartment by a state police officer.[176]

---

170. *Id.* at 500-01.

171. *Id.* A concurring opinion emphasized that Edwards and passengers generally consent to a search, by virtue of the postings at the airports. *Id.* at 504 (Oakes, J., concurring). Other courts have also emphasized this consent notion. *See, e.g.*, United States v. Henry, 615 F.2d 1223, 1230-31 (9th Cir. 1980). *See also* Buchwalter, *supra* note 165, § 2(A)(12).

172. *Id.* at 500.

173. Macwade v. Kelly, 460 F.3d 260 (2d Cir. 2006). Coveny discusses *Macwade* at length, concluding that it may foreshadow a world of little privacy from such government intrusions, largely because the theoretical sufficiency of the "special needs" concept appears to overlook important questions about the utility of such searches and the impact of such searches on privacy. Coveny, *supra* note 156, at 331-34, 364-80.

174. *Macwade*, 460 F.3d at 267-69.

175. A similar analysis was applied by the same court to searches of passengers on Lake Champlain ferries. Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006).

176. United States v. Va Lerie, 385 F.3d 1141 (8th Cir. 2004), *rev'd en banc*, 424 F.3d 694, *cert. denied*, 548 U.S. 903.

The constitutionality of the search seemed to turn on whether the bag had been seized within the meaning of the Fourth Amendment. The court held that it had, consistent with circuit precedent and normal understandings of the meaning of "seizure" under the Fourth Amendment.[177] A dissenting judge argued, however, that such minor relocations should not constitute seizures, specifically noting two factors.[178] First, he reminded the court that the conclusion would necessarily be different at an air terminal, as passenger luggage is controlled and subject to security examination without any concern about whether it has been "seized."[179] Second, he suggested that modern terrorism has changed the public's attitude that any baggage, even first-class checked luggage, is subject to a reasonable expectation of privacy.[180] The judge alluded to the privacy accorded persons and their belongings in air transportation, which has eroded over the decades and is now almost non-existent, presumably forever.[181] The Madrid train attacks, subway attacks in England, and bus attacks in Israel all suggest that any distinction among forms of transportation is unjustified by both logic and experience.[182] The purpose of protecting these common targets from terrorists necessarily translates into broader search powers.

The FISCR now takes the position that FISA searches are constitutional under a special needs analysis. In a 2008 decision considering the validity of provisions in the Protect America Act of 2007, which required communications service providers to assist the government in conducting foreign intelligence electronic surveillance,[183] the court decided that the special needs principle applies by analogy.[184] While the

177. *Id.* at 1146-49.

178. *Id.* at 1151-56 (Riley, J., dissenting).

179. *Id.* at 1156 (Riley, J., dissenting).

180. *Id.* at 1151-56 (Riley, J., dissenting). Both the district court and the dissenting judge on appeal referred to the impact of the September 11 attacks on privacy and government search powers. *See id.* at 1157 n.10 (Riley, J., dissenting).

181. *See id.* at 1157 n.10 (Riley, J., dissenting).

182. *Id.* at 1157 n.10 (Riley, J., dissenting).

183. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified in scattered sections of 18 U.S.C.).

184. *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

court reaffirmed the holding of *In re Sealed Case*, it concluded that the central concern was "the programmatic purpose of the surveillances and whether–as in the special needs cases–that programmatic purpose involves some legitimate objective beyond ordinary crime control."[185] As noted below, the court also recognized the need to consider the totality of the circumstances in order to apply the reasonableness requirement of the Fourth Amendment.[186]

B. *Traditional Dual Purpose Searches*

Fourth Amendment law already acknowledges that government officers will sometimes change or add purposes in the course of their investigations. Much of the case law on special needs searches is based upon this principle in action. While some cases consider the constitutionality of a particular government program in the context of a Fourth Amendment challenge to the program regardless of an attempt by criminal prosecutors to use evidence obtained in the search,[187] most courts address the issue in the context of a motion to suppress evidence obtained during a non-law enforcement special needs search. This was the issue in *T.L.O.*, itself, and at least two of the important Supreme Court decisions concerning roadblocks.[188]

This notion is also the underlying premise of the Plain View Doctrine, under which government officers are permitted to seize evidence that they discover while otherwise acting lawfully.[189] A typical plain view seizure occurs when agents executing a search warrant for one offense discover evidence of a second offense. The central requirement is that the officer is lawfully present where he or she locates the evidence that is

185. *Id.* at 1011.

186. *Id.* at 1012. *See infra* note 221 and accompanying text.

187. *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989) (drug tests of transportation employees) and Michigan Dep't. of State Police v. Sitz, 496 U.S. 444 (1990) (D.U.I. roadblock).

188. New Jersey v. T.L.O., 469 U.S. 325 (1985) (search of personal property to enforce school rules); Illinois v. Lidster, 540 U.S. 419 (2004) (roadblock search for accident investigation); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (border checkpoint search).

189. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.2(a) (4th ed. 2004).

seized.[190] Thus, plain view seizures can occur when officers are performing non-law enforcement functions, such as community-care policing.[191] There is no requirement that the discovery be inadvertent or in any way accidental. Thus, it is entirely permissible for agents to hope and expect to find specific evidence, and then to seize it under the Plain View Doctrine.[192] Viewing this doctrine through the national security purpose that underlies FISA, agents may permissibly "seize" and use evidence of crimes discovered while acting in their foreign intelligence capacity. Just as an officer who notices illegal drugs during a D.U.I. roadblock or while conducting a traffic stop may seize those drugs and use them as evidence in a drug prosecution,[193] so too may the intelligence officer take note of and use evidence of federal crimes committed by targets of FISA authorized electronic surveillance.

The second leg supporting the use of security evidence in criminal prosecutions is that the courts rarely question the motivation of the officers in placing themselves at a location where they can make a plain view seizure. This notion is illustrated by what can be called the Pretense Stop, as illustrated by the facts of *Whren v. United States*.[194] In that case, police officers observed a car committing a moving violation and stopped the car to investigate, presumably in order to issue a citation.[195] As in so many such cases, drugs were observed by the officer during the stop, and a drug seizure and arrest followed.[196] The defendants challenged both the search and the seizure, arguing that the moving violation was

190. *See* Horton v. California, 496 U.S. 128 (1990) (finding that the officer was lawfully present because the search warrant was valid); Coolidge v. New Hampshire, 403 U.S. 443 (1971) (finding that the officer was not lawfully present because the search warrant that was executed was invalid).

191. *See, e.g.*, Cady v. Dombrowski, 413 U.S. 433 (1973).

192. This was the case in *Horton*, in which police officers had a search warrant for the proceeds of a robbery, but failed to also seek a warrant for the weapons used in the crime. The officers expected to seize the weapons, did so, and the courts upheld the seizures under the Plain View doctrine. *Horton*, 496 U.S. at 133-42.

193. *See, e.g.*, New York v. Belton, 453 U.S. 454 (1981); United States v. Robinson, 414 U.S. 218 (1973).

194. Whren v. United States, 517 U.S. 806 (1996).

195. *Id.* at 808-09.

196. *Id.*

so trivial that no reasonable officer would have stopped the car unless motivated to look for evidence of other crimes while at the driver's window, and that therefore, the plain view seizure was a sham.[197] The allegation was credible given the nature of the traffic offense, its location, and the time of night, but the Supreme Court concluded that even if the stop was a pretense, that fact would be irrelevant to any challenge to the validity of the stop.[198] The officers had probable cause of a violation, and therefore, their seizure of the vehicle during the traffic stop was permissible under the Fourth Amendment.[199]

These theories all support the broad use of evidence discovered in FISA-authorized investigations in criminal cases. Stated simply, the argument is that as long as the action was lawful under FISA, it can be redefined as a "special needs" program of searches and seizures, and therefore evidence discovered in "plain view" during a FISA electronic surveillance may be used in criminal prosecutions of any type—even if the investigators were motivated by criminal, rather than intelligence, reasons in conducting their electronic surveillance.

C. *A Different Application of the Special Needs Doctrine*

This is not the only way to read Supreme Court decisions in this area. In some ways, the most applicable Supreme Court decision is *City of Indianapolis v. Edmond*, which involved a challenge to an Indianapolis program of conducting motor vehicle checkpoints in order to prevent illegal drugs from coming into city neighborhoods.[200] These facts are obviously very different from those surrounding foreign intelligence

197. *Id.* at 809.

198. *Id.* at 812-13.

199. *Id.* at 819. The ramifications of *Whren* are potentially quite broad. It seems to allow police officers to shadow suspected criminals and use the full force of arrest and search powers in any matter, no matter how trivial. This notion resonates in the setting of foreign intelligence surveillances, *see infra* Part IV(B)(4), and is consistent with the Bush administration's "spit on the sidewalk" policy that targeted suspected terrorists, *see* ASHCROFT, *supra* note 24, at 124. *See also* LICHTBLAU, *supra* note 122, at 58. The "spit on the sidewalk" reference is to Kennedy's commitment to prosecuting organized crime figures for any and all offenses, including trivial or otherwise rarely prosecuted violations. *See generally* VICTOR S. NAVASKY, KENNEDY JUSTICE 49-107 (1971).

200. City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

searches, but the underlying premise is quite similar. In 1998, the City of Indianapolis decided to conduct checkpoints at various points throughout the city in order "to interdict illegal drugs."[201] Cars were selected through a random process, police conducted brief conversations with the drivers and passengers, and the public was advised that the checkpoints would occur through highly visible public notices posted ahead of time.[202] A six-justice majority invalidated the Indianapolis program.[203] Justice O'Connor's opinion for the Court emphasized several points. First, she noted that all previously approved checkpoints were based on reasons other than law enforcement.[204] These were true "special needs" cases, with objectives such as ensuring safety in transportation, workplace safety at dangerous or highly regulated industries, and protecting the nation's borders.[205] Government searches with the "general purpose of investigating crime" were distinguished, and since Indianapolis had the primary purpose of seizing illegal narcotics before they entered the community, the majority concluded it could not characterize the city's program as containing a non-law enforcement purpose—notwithstanding the obvious public health and safety ramifications of illegal drug use.[206] The Court acknowledged that, at some level of generality, all of the "special needs" settings could be characterized as involving a law enforcement purpose, such as detecting the offense of driving under the influence.[207] In a key passage, the Court distinguished *Whren*, which otherwise would have seemed to be the strongest basis for allowing Indianapolis's program.[208] The Court noted, however, that *Whren* disapproved of looking to the purpose of the search only when there was objective probable cause of a

201. *Id.* at 34.

202. *Id.* at 34-36. The procedures were generally consistent with those upheld in the context of a D.U.I. roadblock in *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990).

203. *Edmond*, 531 U.S. at 33.

204. *Id.* at 37-40.

205. *See id.* at 37.

206. *Id.* at 41 (stating that "[w]e have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing").

207. *Id.* at 42-43.

208. *Id.* at 45.

crime present.[209] Where it is not present, as in the special needs context, courts must examine the programmatic purposes in order to determine whether what had occurred was a legitimate "special needs" search, or a pretext for an unjustified criminal search.[210] The Court also emphasized that a secondary, non-law-enforcement or special needs purpose would not be sufficient to legitimize a roadblock.[211] It acknowledged the validity of security searches such as those conducted at airports and public buildings, but did not suggest that the existence of terrorism in general, or specific connections with international matters, exempted the government's action from these underlying principles.[212]

Edmond is frustrating for scholars and courts trying to evaluate the "purposes" connection between law enforcement and foreign intelligence. In one sense the application of the decision in this setting is problematic. Justice O'Connor's opinion is typical of her style as much as *Keith* was typical of Justice Powell's.[213] The majority opinion never hazarded beyond checkpoints or suspicionless stops, and it gave little indication of the broader canvas in which "special needs" claims are appropriate. The opinion asserted that there is a borderline between the law enforcement purpose of interdicting illegal drugs and the public safety justification of identifying dangerous drivers, but it did not really explain where it lies. It seems likely that the Court would uphold a checkpoint in which officers distribute anti-drug public service brochures or otherwise communicate the dangers of illegal drug use,[214] so

209. *Id.*

210. The Court emphasized that it was the purpose of the general program, implemented by government decision-makers, rather than that of individual officers conducting the checkpoint, that was pertinent. *Id.* at 45-46.

211. *Id.* at 46-47. If so, the Court reasoned, any criminal enforcement roadblock could be made lawful by inclusion of a legitimate special needs aspect, such as a license or sobriety check. *Id.* The Court even left open whether a roadblock with a valid purpose would be legitimate if it also had a secondary purpose of law enforcement. *Id.* at 47 n.2.

212. *Id.* at 47-48. A strong dissent challenged this emphasis on purpose to separate lawful from unlawful checkpoints. *Id.* at 48-56.

213. *See supra* note 38 and accompanying text.

214. This would seem consistent with *Illinois v. Lidster*, 540 U.S. 419, 428 (2004) (upholding a police roadblock conducted in order to locate witnesses of a fatal automobile crash). *See supra* note 160.

the line would appear to illustrate the difference between a strategic approach—the permissible programmatic purpose of decreasing drug use—and the tactical approach—the impermissible case-specific purpose of identifying those transporting illegal drugs.

It would not be surprising to see a five- or even six-justice majority, intent on approving the USA-PATRIOT Act's expansion of FISA authority, treat *Edmond* as of no relevance to FISA electronic surveillance or searches. Still, the decision raises serious questions about the attempts to shoehorn criminal enforcement purposes into foreign intelligence searches. First, there is the need to find the border between law enforcement and other purposes, even if *Edmond* does not define it clearly in that setting. It is hard to characterize the collection of evidence for proof of past crimes as anything other than a law enforcement purpose, which would seem to be consistent with the strategic/tactical distinction identified above. Similarly, if the government in the foreign intelligence sphere is to be free of the traditional strictures of the Fourth Amendment, as FISA provides, it must be because FISA investigations are truly premised on a purpose other than criminal law enforcement.[215] That is, FISA is a federal statutory program for a *non*-law enforcement search, and it is governed by those principles that govern such searches. So understood, the creation of the wall and the need to limit FISA actions to those in which foreign intelligence purposes dominate is unremarkable. If anything, the primary purpose requirement of pre-USA-PATRIOT Act FISA pushes the envelope to some degree, as *Edmond* left open the question of the validity of a checkpoint in which a legitimate special needs purpose was accompanied by a secondary law enforcement purpose. After the USA-PATRIOT Act amendment, FISA now reverses the relationship, purporting to legitimate FISA searches in which the foreign intelligence purpose is "significant," but secondary to a law enforcement purpose.

I argue below that the courts should reject this expansion of FISA. In fact, both the Plain View and Pretense settings

215. This would presumably be dictated by *Keith* because that Court seemed to hold that, while there would be room for Congress to provide different procedures for intelligence investigations, in the criminal realm Title III and traditional Fourth Amendment procedures necessarily apply.

involve legitimate criminal investigative searches, and the Fourth Amendment questions concern only whether additional use may be made of the evidence obtained. In the FISA situation, especially after the USA-PATRIOT Act amendments, the difference is significant. Here the critical fact that permits electronic surveillance (or a physical search) under FISA is that the government's motive is in fact to obtain intelligence of foreign intrigue for intelligence purposes—learning what other nations or terrorist groups are planning to do. Under *Keith*, the constitutional validity of even national security searches subject to the Fourth Amendment would necessarily depend on the purpose actually being foreign intelligence. In a situation in which law enforcement is the dominant motive of electronic surveillance, the far more stringent requirements of Title III of the Omnibus Crime Act should apply. In other words, what makes FISA different in terms of Fourth Amendment requirements should also make it different with respect to using evidence obtained during FISA investigations.[216]

IV. The "Reasonableness" of FISA Searches to Collect Criminal Evidence

A. *The Totality of the Circumstances*

The dominant theme of the last thirty years of Supreme Court jurisprudence on the Fourth Amendment (and much of the Fifth Amendment law as well) is built on the concept of the totality of circumstances. Probable cause is not based on the existence of specific categories of information, as it was for many years.[217] It is based on the totality of circumstances known to the officer or magistrate making the determination in the particular case.[218] Consent to search, probably the most

216. Other reasons for this different treatment of FISA-obtained evidence relate to aspects of the Fourth Amendment that were not really in play at the time of *Keith* and the initial version of FISA. These include changes in territoriality—cutbacks on the reach of the Fourth Amendment and the growth of federal criminal offenses relating to acts in foreign nations. They also include the change in central missions for the Department of Justice and FBI.

217. *See, e.g.*, Spinelli v. United States, 393 U.S. 410 (1969); Aguilar v. Texas, 378 U.S. 108 (1964).

218. *See* Illinois v. Gates, 462 U.S. 213 (1983).

widely used warrant exception, is also based on a totality of circumstances analysis.[219] Perhaps most generally, a totality of circumstances analysis determines both whether a person has been stopped by the police, thereby bringing Fourth Amendment rights into play, and whether there is a reasonable suspicion of a potential crime to justify that stop, and thus be in compliance with constitutional requirements.[220] As noted above, the FISCR has accepted the totality of circumstances methodology for determining the validity of FISA electronic surveillance.[221]

For the most part, the totality of circumstances approach has been a vehicle for scouring the record to identify possible reasons that support police action, reasons that, by themselves, may not amount to much, but, when considered in context with other reasons—i.e., the *totality*—add up to a legitimate basis for a police search or other Fourth Amendment action. Thus, the totality of circumstances framework can be characterized as "police or prosecution-friendly." In the area of dual-purpose foreign intelligence and criminal investigation actions under FISA, however, the totality of circumstances analysis reaches a different result. Here the various circumstances add up to illustrate the *un*reasonableness of allowing the broad use of FISA searches and seizures in criminal investigations that overlap with foreign intelligence operations. There are at least six bases for this argument. In keeping with the totality theme, any of these bases individually would probably not be a convincing reason to deviate from the *Whren*, Plain View, and Special Needs Doctrines, which might support law enforcement use of these intelligence techniques. But two or three, and

219. *See* Schneckloth v. Bustamonte, 412 U.S. 218 (1973).

220. *See, e.g.*, United States v. Cortez, 449 U.S. 411, 417 (1981) (finding that the justifiability of a *Terry*-type seizure or search, like a seizure or search based on probable cause, is supposed to be evaluated on "the totality of the circumstances—the whole picture"); United States v. Mendenhall, 446 U.S. 544 (1980) (plurality opinion) (finding that the stop amounted to a Fourth Amendment seizure) (accepted by majority in INS v. Delgado, 466 U.S. 210 (1984)). Other constitutional tests that depend on the totality of circumstances range from the very common evaluation of the voluntariness of confessions, *see* Dickerson v. United States, 530 U.S. 428 (2000), to the unusual assessment of the use of force to capture a fleeing suspect, *see* Graham v. Connor, 490 U.S. 386 (1989).

221. *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

certainly all six together, make for a different calculation. In context—in totality—these factors support the notion that the Fourth Amendment, and probably rights contained in other constitutional provisions as well, depends on limiting those doctrines to their very different circumstances.

B. *Factors Detracting from the Reasonableness of FISA Searches for Law Enforcement Purposes*

1. The Obvious Purposes and Public Openness of Most Special Needs Searches

One of the reasons that the special needs category of searches works as a variant of traditional Fourth Amendment procedures is that it is usually apparent both that the government's objective is not law enforcement and that criminal evidence is only an accidental, if not always surprising, byproduct of the civil purpose. Thus, agents conduct a roadblock for a public safety purpose, and during that roadblock discover evidence of a crime. It is no stretch to conclude that the roadblock was conducted lawfully, and therefore that use of the evidence derived in a criminal case is equally lawful under the Plain View Doctrine. There are cases where the purposes are not obvious or where there are multiple purposes—and these can cause problems. Still, it is not difficult to conclude that drug testing of individuals in safety or sensitive positions is conducted to ensure that the persons in those positions are drug-free, and not to collect evidence for criminal prosecution.[222] Similarly, roadblocks may be expected to result in identifying some intoxicated drivers who are then subject to criminal prosecution, but the roadblocks are conducted in order to minimize drunk driving through deterrence of the practice rather than through prosecution of criminals.

This seems equally obvious in the classic security search: the airport security gate checkpoint that now includes

222. This is clearly the case with respect to the Supreme Court's leading cases on drug tests. *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989); Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).

mandatory identification checks, metal detectors, x-rays of carry-on belongings, and even virtual strip searches. It is statistically likely that some persons will foolishly carry evidence of a crime through such checkpoints and will be discovered through the searches.[223] But that is far from the purpose, or even a significant purpose, of searches at airport security gates. Rather, air security searches are conducted in order to serve public safety by preventing air piracy or worse. They are open, notorious, and very public.[224] Air travelers necessarily know what will happen to them at security checkpoints, and they know they can avoid discovery of embarrassing items or criminal evidence simply by leaving them at home. Prominent and highly visible signs explain the nature and extent of air security searches and urge persons unwilling to undergo such searches to leave the terminal and travel by other means. In other words, the governmental object of ensuring air safety is served by preventing dangerous passengers from trying anything foolish. When this approach works, there is no evidence to use at trial. In all likelihood, the government will never learn the identity of the potential air pirates.[225]

FISA searches for foreign intelligence activities are necessarily different. Part of the reason is that the government in fact wants to find the very things that will constitute

---

223. There are numerous cases involving drug seizures and quite a few involving weapons. *See, e.g.*, United States v. Dalpiaz, 494 F.2d 374 (6th Cir. 1974) (handgun and knife activated metal detector); United States v. Legato, 480 F.2d 408 (5th Cir. 1973) (heroin discovered in search of package for explosives); People v. Dooley, 134 Cal. Rptr. 573 (Dist. Ct. App. 1976) (narcotics discovered in checked luggage after anonymous call that bomb was on plane was received); Shapiro v. State, 390 So.2d 344 (Fla. 1980) (drugs found during pre-boarding security search); State v. David, 204 S.E.2d 773 (Ga. Ct. App. 1974) (firearm set off metal detector); People v. Brown, 493 N.Y.S.2d 810 (App. Div. 1985) (gun seen in x-ray of briefcase). *But cf.* United States v. $ 124,570 U.S. Currency, 873 F.2d 1240 (9th Cir. 1989) (currency found in illegal search at destination, security justification no longer valid).

224. Some early decisions relied on consent as a theory to uphold searches. *See supra* note 171.

225. The same would seem applicable to drug testing. One of the major points of a drug-testing program is that people subject to the program will avoid using drugs. *See Skinner*, 489 U.S. at 607-09; *Von Raab*, 489 U.S. at 666 ("The purposes of the program are to deter drug use among those eligible for promotion to sensitive positions with the [Customs] Service and to prevent the promotion of drug users to those programs.").

evidence of criminal activity. The objective of FISA searches is to locate proof of foreign espionage or terrorism, which means that the objective is to discover what is usually also evidence of a crime. It asks too much of agents to distinguish between the "objects" to that degree, at least in the absence of clearly defined responsibilities and a wall or something like it. It would be as if Transportation Security Agents were told to look primarily for drugs or counterfeit money, but then expected to justify their searches as based on protecting airplanes and passengers.

More significantly, it is the measure of success that is most revealing of the difference in nature between special needs and FISA searches for criminal evidence. Air security searches are effective largely because by announcing their existence, they prevent most hijackings. The overriding purpose of air safety is served, but it is essentially at the disservice of law enforcement. On the other hand, if passengers and baggage were secretly screened, it is likely that far more evidence of crime would be discovered.[226] But the "special need" of air safety, and the reasonableness of airport security searches under the Fourth Amendment, depends on openness. The fact that national security searches cannot realistically be conducted in the open reveals that the special needs model does not fit very well to justify foreign intelligence searches, even where that is the only purpose.

2. The Extraordinarily Secretive Nature of FISA Searches

In contrast, FISA searches are not just conducted without fanfare in a public arena; they are far more secret than is otherwise tolerated under the Fourth Amendment. Unlike physical law enforcement searches, special needs intrusions, or even Title III electronic surveillance, notice is almost always non-existent or interminably delayed. FISA requires notice to a subject of electronic surveillance only when the government intends to use evidence from that surveillance in a criminal

226. Perhaps air security would be served as well as at present. The answer would probably turn on whether the screening was sufficiently effective to prevent what would in all likelihood be a greater number of air piracy attempts.

prosecution.[227] This may occur years after the electronic surveillance was conducted, or it may never occur. Notice of FISA physical searches[228] is provided only when the residence of a U.S. person is searched, and then, only after the Attorney General "determines there is no national security interest in continuing to maintain the secrecy of the search."[229] In contrast, Title III requires that notice of electronic surveillance be provided within a reasonable time after the end of the surveillance, with a statutory default rule of ninety days after the surveillance ends.[230] The Federal Rules of Criminal Procedure provide that at the conclusion of a physical search, government officers are required to give to a person on the premises (or leave at empty premises) a copy of the search warrant and a receipt for all items taken.[231] The delays and denials of notice under FISA are understandable, even necessary, in many legitimate foreign intelligence investigations. But they seriously undercut any notion that such action is reasonable in what is primarily, or even significantly, a criminal investigation.

The nature of surreptitious physical searches underlines this point. Such searches were virtually unknown until they were used in connection with the installation of oral interception devices—radio transmitters—for electronic surveillance of face-to-face meetings. When approved in that setting, rigid restrictions were imposed to ensure that the secret entry onto private property was not used as an opportunity to search for evidence or even domestic intelligence information.[232] The law remained in that state until the 1995 amendment of FISA to allow surreptitious physical searches.

---

227. 50 U.S.C. § 1806(c) (2006) provides in pertinent part: "Whenever the Government intends to enter into evidence . . . against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial . . . notify the aggrieved person and the court or other authority . . . ." The text makes clear that the evidence could be used in a variety of settings, including state cases. *See id.* § 1806(d).

228. *See supra* Part I(B)(3).

229. 50 U.S.C. § 1825(b).

230. 18 U.S.C. § 2518(8)(d) (2006).

231. FED. R. CRIM. P. 41(f)(1).

232. *See* Dalia v. United States, 441 U.S. 238 (1979) (upholding surreptitious entry order issued in connection with a Title III oral interception order).

Under FISA, searches of private homes may be conducted repeatedly for weeks or months without any judicial finding of probable cause, something that is unimaginable under traditional Fourth Amendment law.[233]

Such secrecy alone would probably not be sufficient to render the loose strictures on foreign intelligence electronic surveillance and physical searches unconstitutional, but it is a factor that weighs heavily in that direction. Without timely notice, there is a much greater intrusion on privacy; with repeated secret entries, there is a much greater intrusion on privacy. Considering these factors, along with others such as the severe restrictions on judicial review, this greater intrusion requires a concomitantly greater justification. It cannot be satisfied by the standards of FISA or other laws that require only a lesser justification.

3. The Problem of Minimal Judicial Review

Many, if not all, of these problems could be remedied by meaningful judicial review. Such review is lacking in FISA.

Judicial review purportedly occurs in two settings. First, it

---

233. Section 213 of the USA-PATRIOT Act amended Section 3103a of Title 18 of the U.S. Code to allow for "delayed notice," formal statutory authority for surreptitious physical searches, in all criminal cases—not just those involving foreign intelligence. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 213, 115 Stat. 272, 285-286 (codified as amended at 50 U.S.C. § 3103a). At least prior to that statute, such "sneak and peak" searches were far more limited and subject to more judicial oversight than FISA surreptitious entry searches. *See, e.g.*, United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

> We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing else. That passion, the true source of the Fourth Amendment demands that surreptitious entries be closely circumscribed. The warrants in this case failed to do so.

Id. *See also* United States v. Villegas, 899 F.2d 1324, 1336-38 (2d Cir. 1990) (imposing a good cause requirement for delaying notice of electronic surveillance).

occurs in the initial authorization of the FISA order. Second, it occurs in litigation in which FISA searches are challenged, most commonly through motions to suppress FISA-based evidence. Yet the judicial role in authorization is limited in several respects. First, as noted above, FISA permits electronic surveillance in the United States in several settings without any judicial role at all.[234] Section 102 of FISA allows warrantless electronic surveillance of non-U.S. persons for as long as one year.[235] Another provision provides for electronic surveillance without prior judicial authorization in an emergency situation.[236] The Bush Administration reportedly found this provision too burdensome and therefore sought additional powers to conduct warrantless electronic surveillance and apparently conducted such electronic surveillance outside of FISA on its own reading of constitutional law.[237] FISA similarly allows physical searches for up to one year on authorization of the Attorney General under similar standards.[238]

Judicial review of FISA applications is also highly limited. Courts simply do not make the sort of decisions they make in criminal cases. Rather, they serve largely as receivers of certifications from the government, such as the certification that a significant purpose of the action is foreign intelligence.[239]

---

234. *See supra* note 61 and accompanying text.

235. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(a)(1), 92 Stat. 1783, 1786 (codified at 50 U.S.C. § 1802(a)(1) (2006)).

236. *Id.* § 105(e), 92 Stat. at 1791-1792 (codified at 50 U.S.C. § 1805(e) (2006)). The section provides in pertinent part that: "[W]hen the Attorney General reasonably determines that . . . an emergency situation exists . . . he may authorize the emergency employment of electronic surveillance . . . ." *Id.* The government must notify a judge and seek judicial approval after the fact. *See id.*

237. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (first report of electronic surveillance outside of FISA). *See also* Anushka Asthana & Karen DeYoung, *Bush Calls For Greater Wiretap Authority*, WASH. POST., Sept. 8, 2006, at A1; Scott Shane & Eric Lichtblau, *Cheney Pushed U.S. to Widen Eavesdropping*, N.Y. TIMES, May 14, 2006, at A1.

238. The general authority to engage in warrantless searches is limited to situations in which it is unlikely that U.S. citizens will be subject to the search. 50 U.S.C. § 1822(a) (2006). The emergency search authority is almost the same as the emergency electronic surveillance provision. *Id.* § 1824(e).

239. *See id.* § 1804(a) (listing the certifications from the Department of Justice); *id.* § 1805(a) (providing that the court must find that the application

The only probable cause requirements are that the target is a foreign power (or an agent of a foreign power) and that the facilities are used by such person or agent.[240] The FISC is not required to find probable cause that the electronic surveillance or search will result in acquisition of foreign intelligence information.[241] This, of course, is a far lower standard than the applicable test in criminal investigations.[242] The judicial approval process is little more than judicial recordkeeping of an executive branch fishing expedition. That may be fine for a true foreign intelligence investigation, but it is not sufficient judicial involvement where the primary purpose of the government's action is to secure evidence for a criminal prosecution.

These limitations on the judicial role in the authorization process might be less of a problem if a judge could fully consider the relevant facts behind an application (or a warrantless search) in the context of later litigation. In other words, if a court had to retroactively decide if in fact there was probable cause to support a search or seizure, the search might be reasonable. FISA provides, however, that the role of the trial judge is more limited. The judge's only role is essentially to see that the paperwork underlying the search was in order.[243]

The key factor making judicial review at this stage fairly shallow is Section 1806(f) of Title 50 of the U.S. Code, which prevents disclosure of FISA documents and requires *ex parte* review in most cases.[244] The history of FISA suppression

---

contains all statements and certifications required by § 1804).

240. *Id.* § 1805(a)(2).

241. Numerous reported cases explain the relative roles of the Department of Justice and the FISC in authorizing electronic surveillance. *See, e.g.*, United States v. Amawi, 531 F. Supp. 2d 832, 834-37 (N.D. Ohio 2008); United States v. Warsame, 547 F. Supp. 2d 982, 986 (D. Minn. 2008); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 301-04 (D. Conn. 2008).

242. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 231-39 (1983) (fair probability that evidence will be discovered). *See generally* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.3 (5th ed. 2009).

243. There is no evaluation of the probable cause of a crime or other textual requirements of the Fourth Amendment, such as reasonable descriptions of the places and items in question. With respect to the key question of probable cause, the only judicial role is in the authorization process, where the judge issuing the order must conclude, in the case of a U.S. person, that the certifications are not clearly erroneous. § 1805(a).

244. Section 1806(f) is a long and complex provision that seems to

hearings reveals that the Department of Justice always files an affidavit stating that national security requires FISA documents remain under seal, that courts always honor these requests, and that the resulting judicial evaluations are ritualistic. For example, in *United States v. Mubayyid*, the court stated:

> It is of course true that the legality of the surveillance and search would be better tested through the adversarial process; an *ex parte* review is not a perfect substitute for that process. The question under the statute, however, is not how to optimize the legal review of the surveillance and search, but whether disclosure is "necessary" in order to make that determination.[245]

The court then addressed the validity of foreign intelligence electronic surveillance in what seems to be a complex federal income tax case, without revealing who, when, where, how often, how long, why, or on what basis the government acted, all in approximately the space of one Federal Supplement page that contained little but *ipse dixit* conclusions.[246] What little we know of government errors in the FISA process comes from

---

provide for *in camera ex parte* review by the court when the government files an affidavit explaining that disclosure, even to the attorneys, would harm national security. *Id.* § 1806(f). In fact, such affidavits appear to have been filed in all cases, and *ex parte* review has always resulted in judicial approval. In other areas of law, national security concerns have been alleviated through careful practices, such as those provided in the Classified Information Procedures Act of 1980, Pub. L. No. 96-456, 94 Stat. 2025 (codified as amended at 18 U.S.C. app. 3, §§1-16 (2006)). *See, e.g.*, United States v. Aref, 533 F.3d 72 (2d Cir. 2008), *cert. denied*, 129 S. Ct. 1582.

245. United States v. Mubayyid, 521 F. Supp. 2d 125, 130 (D. Mass. 2007).

246. *Id.* at 131-32. Numerous courts have upheld electronic surveillance after limited *ex parte* hearings, or else refused to allow disclosure to the defense. *See, e.g.*, *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 165-67 (2d Cir. 2008), *cert. denied*, 2010 WL 58776 (U.S. Jan. 11, 2010); United States v. Abu-Jihaad, 531 F. Supp. 2d 299 (D. Conn. 2008); United States v. Amawi, 531 F. Supp. 2d 832 (N.D. Ohio 2008); United States v. Warsame, 547 F. Supp. 2d 982 (D. Minn. 2008); United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006). *But cf.* El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), *cert. denied*, 552 U.S. 947 (dismissal of civil action under *Bivens* dismissed due to state secrets privilege).

All Matters, where the FISC noted that there had been "misstatements and omissions of material facts" in seventy-five FISA applications, some of which apparently involved intentional misstatements.[247] It seems likely that even more would be discovered in the adversary system generally required for criminal litigation. As it happens, however, the government is allowed to conduct foreign intelligence electronic surveillance under the honor system. It is no wonder that the government prefers to follow FISA rather than Title III in investigations that are primarily criminal in nature.

This minimal judicial role greatly detracts from the reasonableness of the statutory scheme for foreign intelligence searches. It is possible, though far from certain, that such formalistic judicial review is constitutional where the primary purpose of the government's action is to seek foreign intelligence. That, at least, was Congress's intent in enacting FISA. Where, however, the government leaves the legitimate special needs category of foreign intelligence to conduct a search primarily for law enforcement purposes, it is important that the Fourth Amendment not be applied through the very generous lens of foreign intelligence.

4. The Expansion of Federal Criminal Jurisdiction of International and Terrorism Crimes

The Federal Government has increasingly used criminal prosecutions as a vehicle for fighting terrorism. At the time of FISA's enactment, the prevailing notion of the crimes committed by foreign powers was espionage. It is no accident that most of the criminal cases resulting from this era were essentially espionage cases in which successful foreign intelligence electronic surveillance provided evidence that one or more persons were involved in spying on this country.[248] Over roughly the last thirty years, however, Congress has

247. *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002). *See supra* notes 134-36 and accompanying text. Although the court's order was overturned on appeal, nothing in the FISCR's decision questioned the accuracy of the FISC's findings on this point.

248. *See, e.g.*, *Truong*, 629 F.2d 908 (4th Cir. 1980) (Vietnamese spies); United States v. Butenko, 494 F.2d 593 (3d Cir. 1974) (Soviet spies).

enacted a number of statutes that expanded criminal liability for engaging in terrorist activities, expanded criminal law jurisdiction to include extraterritorial actions, and, of course, authorized greater use of investigative techniques to prevent and punish terrorism.[249] A short history of major legislation of the post-FISA period includes enactment of the offense of Hostage Taking as part of an omnibus crime bill,[250] the Omnibus Diplomatic Security and Antiterrorism Act of 1986,[251] the Antiterrorism and Effective Death Penalty Act of 1996,[252] and, of course, the USA-PATRIOT Act.[253] The 1986 law expanded federal power abroad, largely to protect diplomatic personnel and facilities, but it also expanded federal criminal jurisdiction by making it a United States crime to engage in terrorist actions abroad that harm U.S. nationals. That law included a provision that made it unlawful to "kill[ ] a national of the United States, while such national is outside the United States."[254] This has the effect of allowing federal criminal prosecutions for murder or manslaughter that occurs abroad, where terrorists kill U.S. citizens. Abu-Jihaad was charged with violating this law.[255] The 1996 law contained a number of provisions directed at terrorist activities. It significantly added to substantive federal criminal law by including the crime of

249. Some actions occurred earlier. Air piracy became a crime with the Anti-Hijacking Act of 1974, Pub. L. No. 93-366, 88 Stat. 410, *amended by* Pub. L. No. 103-272, 108 Stat. 1241 (codified as amended at 49 U.S.C. § 46502 (2006)). This is consistent with the rash of airplane hijackings of the period.

250. Act for the Prevention and Punishment of the Crime of Hostage Taking, Pub. L. No. 98-473, § 2002, 98 Stat. 1837, 2186 (codified as amended at 18 U.S.C. § 1203 (2006)).

251. Omnibus Diplomatic Security and Antiterrorism Act of 1986, Pub. L. No. 99-399, 100 Stat. 853 (codified in scattered titles of the U.S.C.).

252. Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of the U.S.C.).

253. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, Pub. L. No. 107-56, tit. II, § 218, 115 Stat. 272, 291 (codified as amended at 50 U.S.C. §§ 1804, 1823).

254. Omnibus Diplomatic Security and Antiterrorism Act of 1986, § 1202, 100 Stat. at 896 (codified at 18 U.S.C. § 2332(a) (2006)).

255. Indictment, *supra* note 1, at ¶ 29. Mayfield was apparently arrested as a material witness to terrorism offenses in Spain. *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1026-29 (D. Or. 2007), *vacated*, 588 F.3d 1252 (9th Cir. 2009).

"providing material support for terrorist organizations."[256] Professor Norman Abrams points out that "most of the prosecutions initiated since September 11, 2001 have involved offenses and related provisions enacted in the 1996 Act."[257]

The emphasis of the USA-PATRIOT Act, on the other hand, was in expanding investigative powers and techniques. In addition to allowing the use of FISA for investigations in which foreign intelligence is a significant, but not primary, purpose, the law included provisions that eased restrictions on the use of pen registers and access to internet communications,[258] loosened grand jury secrecy in the foreign intelligence area,[259] and expanded the scope of subpoenas for records and tangible evidence.[260] Other laws, including a series of laws intended to permit greater executive use of electronic

256. Antiterrorism and Effective Death Penalty Act of 1996, § 323, 110 Stat. at 1255, *amending* Pub. L. No. 103-322, § 120005(a), 108 Stat. 1796, 2022 (codified as amended at 18 U.S.C. § 2339A (2006)). The provision provides, in pertinent part, that "[w]hoever provides material support or resources or conceals or disguises the nature, location, source, or ownership of material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, a violation of [numerous sabotage and terrorism-related offenses]." § 2339A(a). *See also id.* § 2339B (2006) (Providing Material Support or Resources to Designated Foreign Terrorist Organizations).

257. NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT 10 (3d ed. 2008). This book contains an extended and informative discussion of federal legislative efforts during this period. *See id.* at 6-48. Well-known prosecutions for these offenses include *United States v. Hammoud*, 381 F.3d 316 (4th Cir. 2004) (money laundering and material support conviction related to Hizballah); *United States v. Sattar*, 314 F. Supp. 2d 279 (S.D.N.Y. 2004) (prosecution of New York criminal defense attorney Lynne Stewart for passing messages to and from convicted terrorist leader); Indictment, *United States v. Lindh*, No. CR 02-37-A (E.D. Va. Feb. 2002), *available at* http://news.findlaw.com/hdocs/docs/lindh/uswlindh020502cmp.html.

258. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, § 214, 115 Stat. at 286 (codified as amended at §§ 1842-1843 (2006)) (Pen Registers and Trap and Trace Authority Under FISA); *id.* § 215, 115 Stat. at 287-88 (codified as amended at § 1861 (2006)) (Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations).

259. FED. R. CRIM. P. 6(e)(3)(D) (Authority to Share Criminal Investigative Information).

260. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA-PATRIOT) Act of 2001, § 210, 115 Stat. at 283 (codified as amended at 18 U.S.C. § 2703 (2006)) (Scope of Subpoenas for Electronic Communications); *id.* § 215, 115 Stat. at 287-88 (codified as amended at 50 U.S.C. § 1861 (2006)).

surveillance, have been passed since 2001.[261] These and other statutes have provided various legal tools, such as executive orders, to designate organizations as terrorist organizations and to freeze assets of such groups.[262]

Before this great expansion of both federal criminal jurisdiction and civil and criminal vehicles for fighting terrorism, it was reasonable to think of foreign intelligence as primarily directed to international politics, diplomacy, and war, with criminal prosecution an ancillary part of the government's efforts against foreign espionage and terrorism. Now criminal prosecution is clearly a major part of a very big toolbox. The cost of making criminal prosecution such a central part of the government's efforts in this area is that, where prosecution rather than intelligence-gathering is the primary purpose of electronic surveillance or physical searches, it may well be that the government has to follow the procedures laid down by the Constitution for the investigation and prosecution of criminal cases.

5. FISA Searches are Extremely Intrusive, Especially Compared to most Special Needs Searches

No one can doubt that the electronic surveillance and physical searches authorized by FISA are extremely intrusive on personal privacy. Electronic surveillance has been recognized as among the most invasive of government investigative techniques since *Berger v. New York*,[263] where the Court stated: "Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[264] The Court was equally clear in *Keith*:

---

261. *See, e.g.*, USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections of the U.S.C.); Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified in scattered sections of 50 U.S.C.); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of the U.S.C.).

262. *See, e.g.*, Chai v. Dep't of State, 466 F.3d 125 (D.C. Cir. 2006) (reviewing Secretary of State's order designating organization as a Foreign Terrorist Organization); Global Relief Found. v. O'Neill, 315 F.3d 748 (7th Cir. 2002) (reviewing Secretary of Treasury's order freezing assets).

263. Berger v. New York, 388 U.S. 41 (1967).

264. *Id.* at 63.

> There is, understandably, a deep-seated uneasiness and apprehension that this [electronic surveillance] capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.[265]

Interceptions of telephone conversations or face-to-face meetings, and physical invasions of a person's home, even with a warrant, are frightening and degrading and a strong reason for the prominence of the Fourth Amendment in constitutional text and history.

Two additional aspects of FISA searches illustrate the fact that their impact is unmatched among generally lawful intelligence-gathering activities. First, the lack of a criminal probable cause requirement opens the door to government action based on general notions of subversion, disloyalty, or vocal policy disagreement. It is for this reason that FISA explicitly provides 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."[266] While this should help protect many within the class of U.S. persons, the need to include it proves the potential threat to liberties. Here again the *Keith* Court was direct:

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of

265. *Keith*, 407 U.S. 297, 312-13 (1972).

266. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105, 92 Stat. 1783, 1790 (current version at 50 U.S.C. § 1805(a)(2)(A) (2006)). *See* Kreimer, *supra* note 28 (concerning the extent to which political views have affected surveillance targeting in the past).

> the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.[267]

Second, FISA searches are exceptionally lengthy. Electronic surveillance can be authorized for a year, and extensions are possible;[268] the same authorization periods apply even to physical searches.[269] In contrast, electronic surveillance orders in criminal investigations can only be valid for up to thirty days.[270] Under typical search law, a physical search occurs once, within fourteen days of the issuance of the search warrant.[271]

The question of surreptitious searches raises other questions that arise only in rare and extreme criminal cases. A search authorization for ninety days, without notice at that time to the owner or occupant, and without the purpose of seizing tangible evidence, is obviously an authorization for one or more secret searches. Secret searches are by definition more intrusive on personal freedom and security than even a full-scale item-by-item police search. The fear of being subject to such continued violations, and the possibility of learning about them only months or years after the fact, are unquestionably severe invasions of Fourth Amendment interests.[272] The facts of *Mayfield* illustrate some aspects of the intrusion on both his rights and those of his family:

> The family's most intimate conversations were recorded. They were followed. When the FBI

---

267. *Keith*, 407 U.S. at 320.

268. *See* Foreign Intelligence Surveillance Act of 1978, § 102(a)(1), 92 Stat. at 1786 (current version at 50 U.S.C. § 1802(a)(1) (2006)) (concerning warrantless orders). *See also id.* § 105(d)(2), 92 Stat. at 1790 (current version at § 1805(d)(2)) (concerning court orders).

269. *See* 50 U.S.C. § 1822(a)(1) (2006). *See also* § 1824(d)(2).

270. *See* 18 U.S.C. § 2518(5) (2006).

271. *See* FED. R. CRIM. P. 41(e)(2)(A)(i).

272. *See generally* Robert Duncan, *Surreptitious Search Warrants and the USA Patriot Act: "Thinking Outside the Box But Within the Constitution," or a Violation of Fourth Amendment Protections?*, 7 N.Y. CITY L. REV. 1 (2004).

> thought the Mayfields were not at home or at work, FBI agents on multiple occasions surreptitiously entered their house and law office, looking at and copying their personal and private documents, legal files and computer hard drives. The government admits that over 300 photographs were taken inside the Mayfield home, and additional photographs inside Mr. Mayfield's law office.[273]

The intrusive effect of FISA electronic surveillance and searches is in stark contrast to the sort of intrusion permitted in most special needs cases. As Professor Dressler notes, police officers rarely conduct special needs searches; instead it is usually civilian, non-law-enforcement employees, who lack the intimidating appearance of armed officers.[274] Courts upholding special needs searches often stress that the search was not excessively intrusive,[275] or involved only a minimal privacy interest.[276] The Supreme Court has repeatedly emphasized that a search was reasonable in part because it was short in duration.[277] Special needs searches are often very limited, looking only for specific items, thus the searches are closely tailored to fit that special need. The attempt to expand the special need of foreign intelligence to encompass searches primarily directed to law enforcement completely undercuts the principle, and therefore undercuts this rationale for exemption from standard Fourth Amendment requirements.

---

273. Memorandum in Support of Plaintiff's Motion For Summary Judgment, Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (No. CV-04-1427-AA), 2007 WL 834254, at *1. Although this was the plaintiff's memorandum, these matters were in the stipulation of facts between Mayfield and the government.

274. JOSHUA DRESSLER & ALAN MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE 328 (4th ed. 2006).

275. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 726 (1987).

276. *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 624-26 (1989).

277. *See, e.g.*, Illinois v. Lidster, 540 U.S. 419, 425 (2004); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 452 (1990); United States v. Martinez-Fuerte, 428 U.S. 543, 558 (1976).

6. The Hardship to the Government is Largely Illusory

The implication, by those who support the USA-PATRIOT Act's expansion of FISA, is that modification was necessary in order to allow intelligence officers to "connect the dots."[278] This claim does not withstand analysis. No one has suggested, let alone proved, that appropriate foreign intelligence actions were prevented by the primary purpose requirement or the wall that the Department of Justice developed to show that its FISA investigations were in fact motivated by foreign intelligence objectives. Statistics indicate that FISA orders have increased somewhat over the last decade,[279] but there is no reason to believe that this results from use of FISA for what are primarily criminal investigations. Logic suggests that the increased use of FISA has resulted largely from the increased human and material resources devoted to the war on terrorism after the September 11 attacks. Unless and until anyone can prove that worthwhile foreign intelligence investigations had to be derailed due to the primary purpose requirement, it is hard to give credence to claims that the requirement imposes a serious burden on legitimate intelligence investigations.[280] In fact, if the intelligence officials were making good choices about targets, and government attorneys were reasonably interpreting FISA and the Fourth Amendment, the only FISA searches that should have been prevented by the primary

278. *See, e.g.*, ASHCROFT, *supra* note 24, at 144-56 (criticisms of the wall).

279. Electronic Privacy Information Center, *supra* note 152.

280. The only specific example of such an occurrence in the large body of writing on intelligence matters over the last several decades does not provide much support. Victoria Toensing, a Deputy Assistant Attorney General in the President Reagan Justice Department, has written that she terminated a FISA wiretap during an air hijacking on advice from career attorneys. The attorneys were apparently concerned that remaining on a wiretap of associates of the hijackers prevented the tap from being primarily for foreign intelligence purposes. *See* Kris, *supra* note 112, at 501. Putting aside the fact that this decision took place long before the sorts of rigid procedures derided as "the wall," it reveals only bad lawyering by political and career Justice Department attorneys. An otherwise legitimate foreign intelligence wiretap that provides information helpful in ending a terrorist event is self-evidently a foreign intelligence wiretap. The intention and use are both to learn about and resolve a terrorist event—plainly an intelligence purpose. The use of information in the resulting criminal prosecutions is the sort of secondary use of information anticipated by FISA and the courts that have considered criminal cases using FISA evidence.

purpose requirement would be those primarily directed at collecting evidence against U.S. persons for criminal prosecution. Unless we change the Fourth Amendment, our system treats that as a tolerable burden.[281]

In the end, that is what the Special Needs Doctrine seems to be about. The policies underlying programmatic searches, from drug tests to D.U.I. roadblocks to foreign intelligence electronic surveillance, are debatable and require legislative rather than judicial oversight. If those policies are sufficiently compelling, and the burdens on individuals comparatively light, it makes sense for courts *not* to bring into play the full panoply of Fourth Amendment requirements. But the cost to the public of the government obtaining search and seizure powers without meeting those requirements is that it must avoid conducting its criminal investigations using those enhanced foreign intelligence powers.

If the price of robust powers to protect the nation is that the government bend over backwards to avoid using criminal law remedies, it is a price worth paying. There are many examples of governments having to forego criminal prosecutions because of choices made at the investigative stage. Some involve typical criminal justice system actions, such as grants of immunity. Others, more applicable to the current international scene, result from government actions that include overly aggressive tactics, such as harsh interrogations, in which the resulting evidence may be inadmissible in court. Sometimes criminal cases are quashed because of other legal or political realities, such as where Diplomatic or Consular Immunity prevents prosecution, or spies are traded back to their own nations. Insisting on the legality of electronic surveillance without probable cause, and in some cases without

281. In the end, this is not really much about the exclusionary rule. Whether courts decide to permit or exclude evidence obtained for criminal cases is largely beside the point. As in most other special needs settings, the real issue is the extent to which the government may engage in searches or seizures, and the underlying question is the permissibility of the program, rather than the treatment of the resulting evidence. If the government follows the primary purpose test, as it presumably did from 1978 to 2001, however, there would not even be a question about the admissibility of the resulting evidence because doctrines such as the Plain View doctrine, *see* discussion *supra* notes 189-93, and cases such as *Illinois v. Lidster*, 504 U.S. 419 (2004), *see supra* note 214, plainly allow the use in criminal prosecutions of evidence obtained in special needs cases.

warrants, in order to achieve criminal law enforcement purposes runs the real risk that the techniques will be marked off-limits, even for intelligence purposes, because it can no longer be stated with confidence that the searches are reasonable, special needs searches.

The wall, as developed over several presidential administrations and as revised by the FISC in 2002, really served to enhance government power. Its existence allowed the intelligence agencies to operate, confident that they could prove that their investigations were motivated by the need for foreign intelligence. At the same time it allowed the Department of Justice to use the results of FISA searches in criminal prosecutions. In a sense, the wall allowed the government to prove that its foreign intelligence searches were in fact special needs searches. It cannot do so today.

V. Conclusion: The New Paradigm and the Limits of Precedent

One year into the Obama Administration, there is no indication that the Department of Justice has ended John Ashcroft's New Paradigm. Apparently, we can expect the Department to continue to emphasize prevention of terrorism over the prosecution of crime. Since the government is still likely to move aggressively against international terrorists in federal criminal prosecutions, the dual purpose foreign intelligence/law enforcement search is likely to be with us for some time.

As long as intelligence and prevention are the first objects of the Department, there must be some workable set of rules to make sure that the New Paradigm does not obliterate the probable cause and warrant requirements—the default settings of the Fourth Amendment. It is not acceptable to adopt a pure "reasonableness" requirement and then to rubber stamp as reasonable each and every intrusion that seems to serve short-term needs. The lightweight version of the Fourth Amendment contemplated by the Special Needs and other various doctrines, which allow very intrusive searches without the traditional protections of the Fourth Amendment, are controversial enough in their own right and are plainly inadequate when purposely used to enforce criminal law. The "special needs" Fourth Amendment exists only because it is outside the

criminal law system. Its application in the criminal law system is thus a serious error of constitutional criminal procedure and a potential disruption of the complex set of doctrines that have grown up to permit government searches in appropriate non-criminal cases. The wild card of the "significant purpose" rule is as likely to result in a narrowing of foreign intelligence powers or, more generally, in special needs authority, as it is to result in approving enhanced authority to search in quasi-criminal matters.

Despite the bromides directed at the wall's arguable effect of shutting down some intelligence sources, it has largely served to keep the criminal justice system out of the way of the intelligence gathering system, and vice versa. To take the anecdotal example of the unwillingness of the FBI to share data concerning flight training by suspected terrorists before the September 11 attacks, is it really likely that such obviously pertinent intelligence information was somehow kept from intelligence officers by the wall? The information was intelligence, not criminal evidence. It only became criminal evidence after the intelligence system failed and there was a crime to investigate. If the information had been shared there might never have been September 11 attacks, and if they had still occurred, the use of intelligence information in any resulting criminal prosecution would be patently lawful. Any dot-connecting flaws were due to the lack of coordination within the intelligence community.[282] No problems resulted from applying the Fourth Amendment's requirements to those investigations in which law enforcement, rather than foreign

282. Stated differently, the wall should not be blamed for the failure of government officials to implement it effectively. The recent history of the period reveals that inadequate resources were provided to the agencies, the data management was mid-20th century, and good-old bureaucratic turf protection was in full force. In the wake of the September 11 attacks, Attorney General Ashcroft identified a lack of political will and inadequate technology as major causes. ASHCROFT, *supra* note 24, at 244. The failure to share information competently within intelligence agencies remains a critical problem, as revealed by the events leading up to the attempted Christmas 2009 "underwear" bombing. *See* Peter Baker & Carl Hulse, *Obama Hears of Signs that Should have Grounded Plot*, N.Y. TIMES, Dec. 30, 2009, at A1; Karen DeYoung, *Bombing Reports Start Trickling In to Obama*, WASH. POST, Dec. 30, 2009, at A3; Doyle McManus, Op-Ed., *Another Failure to Communicate, 9/11 was Supposed to be a Wake-Up Call For U.S. Intelligence Agencies. Nope.*, L.A. TIMES, Jan. 3, 2010, at 26.

intelligence, was the dominant purpose.[283]

In the end, the problem of using investigative techniques against potential terrorists to obtain foreign intelligence and to collect evidence of crimes illustrates one of those law school conundrums—the limits of building logically on precedent. Here, it is possible to take several minor steps and see them lead fairly clearly in the direction of allowing the use of broad and largely unregulated tactics against potential sources of foreign intelligence in order to obtain evidence that would be useful and probably admissible in criminal prosecutions. This is what the FISCR did when it concluded in 2002 that the Special Needs Doctrine allowed such searches. The logical components, however, lead to an illogical conclusion. In fact, the minor steps obscure that the fundamental requirement is reasonableness, and what is reasonable can depend on a number of factors, not just to the extent it furthers the goal of foreign intelligence.

The reasonableness "totality of the circumstances" test has long been a central part of Fourth Amendment law, and by definition, serves to prevent abstract theories from building up a superstructure that ignores context, impact, and the practical aspects of both intelligence and criminal investigations. In a sense, this is the message of *City of Indianapolis v. Edmond*.[284] If the purpose of the investigation is something other than law enforcement, then application of traditional law enforcement aspects of the Fourth Amendment seems beside the point. Instead, courts seek a common sense accommodation of the competing interests and apply it to the intrusion. But where there is a significant law enforcement purpose, traditional rules must apply. Otherwise, there would be no limits to mandatory drug tests, roadblocks, and presumably house-to-house and car-to-car searches—all for any of a number of combined law enforcement and "special needs" purposes. The attempt in the USA-PATRIOT Act to end-run these principles by allowing extremely aggressive searches where a

283. And even if they were, we would all be happier now if the officials in question had recognized that the national security interest was in fact dominant, disclosed the information as required by public safety, and let the chips fall where they may.

284. City of Indianapolis v. Edmond, 531 U.S. 32 (2000). *See supra* notes 200-14 and accompanying text.

"significant" purpose is foreign intelligence simply turns *Edmond* on its head. It purports to allow a secondary or tertiary intelligence purpose to override the dominant law enforcement purpose in many cases. On top of that, it allows the most intrusive sorts of searches, and those that are most likely to turn up evidence of crimes. We do not know how many FISA searches or other intelligence investigations are flawed in this fashion. It may be very few, which would support the argument that returning to the wall and the primary purpose requirement would cause little disruption to national security. It may be more than a few, which would support the argument that greater care should be taken to ensure that the government is not permitted to get around the Fourth Amendment in criminal cases by invoking the *deus ex machina* of foreign intelligence. The wall, with its insistence that foreign intelligence searches be justified by *foreign intelligence* justifications, protects us and still allows appropriate government searches to continue.

But I hold no confidence in the power or the will of most courts to insist that the government turn square corners in this respect. The political pressure to do nothing that appears to make intelligence-gathering or criminal prosecution more difficult is seemingly too much to resist, apparently even for judges with lifetime tenure, and even where the added burden on intelligence investigations is almost entirely ephemeral. The Supreme Court of 1973, which decided *Keith*, however, would not have allowed this to occur. Perhaps someday, especially if the present Supreme Court stays out of this controversy and issues no binding precedents, future judges will recognize that the central meaning of the Special Needs Doctrine, along with statutory requirements such as minimization rules, provide an authoritative path to maintaining as much separation between foreign intelligence and criminal investigations as is feasible.