Article

The Death of FISA

William C. Banks†

Introduction 1209
I. The Origins of FISA 1211
II. Foreign Intelligence Surveillance Act Practice Up to September 11 1211
III. The Post-September 11 Changes 1211
A. The Collapse of the Foreign Intelligence Purpose Rule 1211
B. Avoidance of FISA: The Terrorist Surveillance Program 1211
C. Synthesizing the Post-September 11 Developments: The Death of FISA 1211
1. The Wall 1211
2. Statutory Obsolescence and Lone Wolf 1211
IV. The Future Prospects 1211
A. FISA and Modern Technology 1211
B. Is the TSP Lawful? 1211
C. Proposals to Amend FISA 1211
D. Can FISA Be Saved? 1211
1. Minimization Reforms? 1211
2. An Exclusionary Rule for FISA? 1211
3. Improved Oversight of FISA Activities 1211
E. Revisions to FISA to Accommodate the TSP 1211
Conclusion 1211

Blinded by dizzying technical advances in surveillance, and by the politics of the post-September 11 emergency, Congress

† Laura J. and L. Douglas Meredith Professor, Director, Institute for National Security and Counterterrorism, Syracuse University. Special thanks for helpful comments to M.E. (Spike) Bowman, Bobby Chesney, Peter Raven-Hansen, Kim Taipale, and the participants in the 2006 Minnesota Law Review Symposium, "9/11 Five Years On: A Look at the Global Response to Terrorism." Excellent research assistance was provided by Jesse Blinick.

appears poised to grant the twenty-first century equivalent of eighteenth century general warrants[1]—allowing the executive to conduct national security surveillance at will. Even if Congress does not grant such sweeping discretion by statute, arguably the modern general warrant is with us now, by order of the President. Just as English law permitted the searcher to "'break into any shop or place suspected,'"[2] the executive branch has invoked the specter of additional terrorist attacks against the United States to justify sweeping electronic surveillance of Americans, without judicial approval and outside the bounds of any statute.[3] Within days of September 11, Attorney General John Ashcroft stated that the Department of Justice would thereafter be guided by a "paradigm of prevention," or preventive enforcement, where every resource would be devoted to early anticipation of potential terrorism plots.[4] Over the last five years, the determination that the United States cannot wait until terrorist plots are fully developed and operational before they are stopped has become an established part of the counter-terrorism landscape,[5] while the rise of preventive enforcement as a preferred counter-terrorism approach is a dominant theme in the Department of Justice strategy statements.[6]

1. General warrants were given to agents of the Crown, permitting wholesale ransacking of the homes and businesses of political opponents. Following a history of such abuses under Charles I, the courts struck down general warrants and Parliament proscribed them a year later. *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 2–4 (2000).

2. William Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 381 (1980) (quoting Copy of Council Order, July 30, 1621, Earl de la Warr collection, *in* FOURTH REPORT OF THE ROYAL COMMISSION ON HISTORICAL MANUSCRIPTS 312 (London, 1874)).

3. U.S. DEP'T OF JUSTICE, REDESIGNING DOJ TO PREVENT FUTURE ACTS OF TERRORISM: RESHAPING THE FBI'S PRIORITIES TO FOCUS ON ANTI-TERRORISM (May 29, 2002), http://usinfo.state.gov/is/Archive_Index/Redesigning_DOJ_to_Prevent_Terrorism.html (noting the extensive preventive measures taken in response to the threat of terrorism).

4. *See id.*

5. *See, e.g.*, U.S. SENATE SELECT COMM. ON INTELLIGENCE & U.S. HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351 & H.R. REP. NO. 107-792, at 33 (2002) (noting key failures in preventative measures prior to the September 11 attacks); Editorial, *The Limits of Hindsight*, WALL ST. J., July 28, 2003, at A10.

6. *See* U.S. DEP'T OF JUSTICE, FACT SHEET: DEPARTMENT OF JUSTICE ANTI-TERRORISM EFFORTS SINCE SEPT. 11, 2001, No. 06-590 (Sept. 5, 2006)

One of the most useful tools available to the government to learn about terrorist plans before they mature has been the Foreign Intelligence Surveillance Act (FISA).[7] Whether the strategy is to arrest the targets of surveillance early, or to continue monitoring in the hopes that more serious and sophisticated terrorists might enlist others as decoys or assets in a more concrete and more nearly operational plot, FISA permits the government to keep tabs on the targets without their ever knowing about the surveillance.[8]

Enacted in 1978, FISA resulted from an inter-branch compromise. Until then, no president had ever conceded that the Congress could interpose any set of procedures to confine the constitutional discretion of the president to engage in electronic surveillance to protect the national security.[9] However, beginning in the 1960s, the Supreme Court recognized an emerging constitutional right of privacy that is implicated when government conducts electronic surveillance, and courts began to limit warrantless electronic surveillance.[10] Soon thereafter, the Wa-

[hereinafter DOJ, FACT SHEET], *available at* http://www.usdoj.gov/opa/pr/2006/September/06_opa_590.html; Alberto R. Gonzales, U.S. Att'y Gen., Prepared Remarks of Attorney General Alberto R. Gonzales at the World Affairs Council of Pittsburgh on Stopping Terrorists Before They Strike: The Justice Department's Power of Prevention (Aug. 16, 2006), *available at* http://www.usdoj.gov/ag/speeches/2006/ag_speech_060816.html ("[W]e need to gather enough information and evidence during our investigations to ensure a successful prosecution, but we absolutely cannot wait too long, allowing a plot to develop to its deadly fruition."); Paul J. McNulty, U.S. Deputy Att'y Gen., Prepared Remarks of Deputy Attorney General Paul J. McNulty at the American Enterprise Institute (May 24, 2006), *available at* http://www.usdoj.gov/dag/speech/2006/dag_speech_060524.html ("The death and destruction of September 11, 2001 mandate a . . . preventative approach.").

7. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1862 (2000 & Supp. II 2002)). FISA also prescribes the rules for collecting foreign intelligence information in the United States. *See* 50 U.S.C. § 1801(f). The Act thus has no bearing on the United States' authority to conduct intelligence collection outside the United States. Although FISA procedures may be employed to conduct physical searches, this Article examines only the portions of FISA regulating electronic surveillance in the United States.

8. *See id.* §§ 1801–1862.

9. *See* Banks & Bowman, *supra* note 1, at 75 (noting that even in 1976, President Ford was attempting to submit a bill that would codify current executive branch practices).

10. *See* Katz v. United States, 389 U.S. 347, 359 (1967), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-351, 82 Stat. 212, *as recognized in* United States v. Koyomejian, 946 F.2d 1450, 1455 (9th Cir. 1992) (applying the Fourth Amendment warrant provision to electronic surveillance).

tergate scandal and follow-on investigations of surveillance abuses by the Nixon administration and the administrations of earlier Presidents emboldened Congress and persuaded Presidents Ford and Carter to work toward a legislative scheme permitting secret electronic surveillance for foreign intelligence while providing for judicial involvement and congressional oversight to assure Americans that past abuses would not be repeated.[11]

Five years after the September 11 attacks, FISA unraveled following the amendments to FISA made at the insistence of the executive branch.[12] A series of events led to this state of affairs. September 11 created an aura of emergency in the government, and the emergency and its politics determined a range of policy and law developments. Congress essentially ceded its role in crafting legislation and in national leadership, while the executive branch seized the initiative to fight the global war on terrorism at home and abroad with the tools it could fashion. With a few notable exceptions,[13] the courts have also been sensitized to the emergency.[14]

Meanwhile, even though the failures to share information before September 11 did not stem from inadequate authorities or from legal obstacles, inter-agency finger-pointing at the failure to stop the hijackers[15] led to changes in the law to encour-

11. S. REP. NO. 95-604, pt. 1, at 8–9 (1976), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3909–10.

12. *See* discussion *infra* Part III.A–B.

13. *See* Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2759 (2006) (finding that the military commissions established by presidential order violated congressional statutory restrictions); Hamdi v. Rumsfeld, 124 S. Ct. 2633, 2648 (2004) (holding that courts may inquire into the factual basis for the President's detention of a U.S. citizen as an enemy combatant); Rasul v. Bush, 124 S. Ct. 2686, 2698 (2004) (holding that the federal district court had habeas corpus jurisdiction over Guantánamo Bay detainees' lawsuits and rejecting the argument that it would be unconstitutional to interpret the statute to infringe upon the President's powers as commander in chief).

14. *See* Padilla v. Hanft, 423 F.3d 386, 397 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1649 (2006) (upholding the military detention of a U.S. citizen who was detained upon entering the United States unarmed and held in civilian custody at the time of military detention); MacWade v. Kelly, No. 05CIV6921RMBFM, 2005 WL 3338573, at *20 (S.D.N.Y. Dec. 7, 2005), *aff'd*, 460 F.3d 260 (2d Cir. 2006) (upholding based on compelling need a random container inspection program for New York City subways used to deter terrorist attacks).

15. *See September 11 and the Imperative of Reform in the U.S. Intelligence Community: Hearing Before the H. Select Comm. on Intelligence*, 107th Cong. 29 (2002) (statement of Sen. Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence), *available at* http://intelligence.senate.gov/shelby

age information sharing.[16] In 2002, relying on post-September 11 changes to FISA that loosened the requirement that "the purpose" of FISA surveillance is pursuit of foreign intelligence,[17] the Department of Justice furthered the dismantling of one component of the 1978 FISA compromise—the "wall" procedures which ensured that prosecutors would not build their cases upon or have their cases tainted by unlawfully obtained evidence.[18] A special court of appeals gutted this central premise of FISA when it upheld the Department's new procedures permitting the use of FISA even when the primary objective of the planned surveillance is to find evidence to support a prosecution.[19]

At the same time, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act)[20] and rewritten FBI guidelines[21] modernized FISA to account for new technologies and changing tactics in the never-ending leap-frog of the technologies of detection and evasion.[22] Despite the Bush administration's proclaimed satisfaction with the new tools, they secretly circumvented the updated FISA procedures in undertaking a new domestic surveillance program through the National Security Agency (NSA)—the Terrorist Surveillance Program (TSP). Although strong negative reactions followed the media release of the NSA story in December 2005,[23] the administration has made legal arguments to justify not follow-

.pdf [hereinafter *Hearing*] (detailing the missed opportunities to share available information about the al Qaeda threat inside the United States before September 11).

16. William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1166 (2003).

17. Part III.A., *infra*, considers the effect of the change from "the purpose" to "a significant purpose" in FISA.

18. Banks, *supra* note 16, at 1167–68.

19. *In re* Sealed Case, 310 F.3d 717, 720, 746 (FISA Ct. Rev. 2002), *cert. denied*, ACLU (2003).

20. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act (Patriot Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified at 50 U.S.C. §§ 1801–1862).

21. JOHN ASHCROFT, U.S. ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS (May 30, 2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf.

22. *See* discussion *infra* Part IV.A.

23. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

ing FISA while it supports amendments to the act that would eviscerate it.[24] The administration has repeatedly stated that the TSP is limited to situations where one end of the communications captured is a known or reasonably suspected affiliate of al Qaeda, but those assurances are not subject to independent verification outside the executive branch.[25] In any case, if the TSP can work around FISA for one programmatic purpose, it would be difficult to stop other such evasions of the FISA scheme. One way or the other, it looks like FISA is dead.

This Article is a requiem for FISA, and a plea for our government to restore the constitutional values that FISA wisely straddled—promoting national security while safeguarding civil liberties. FISA may have been doomed from the start because of its complex formulations regarding who the government may target, how the government must construct the applications, and how the government must minimize its dissemination of information collected. Still, its core set of requirements, and the judicial procedures to enforce them, remained in place until 2002.[26] Even before September 11, and exponentially more so since then, a growing criminalization of terrorism-related activities has made the prosecutorial agenda a larger part of the sphere of electronic surveillance, and has accordingly further complicated the task of managing FISA implementation.[27] With the long list of amendments enacted in the Patriot Act in 2001, and some others before and since then, the original deal from 1978 may have collapsed under its own weight. Whether from its cumulative complexity, the challenges of new technologies, or the efforts of the Bush administration after September 11 to curtail and circumvent its provisions, the

24. *See* Letter from William E. Moschella, U.S. Assistant Att'y Gen., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. 3 (Dec. 22, 2005), *available at* http://www.usdoj.gov/ag/readingroom/surveillance6.pdf (arguing that presidential actions were excepted from FISA "procedures"). The proposed amendments to FISA supported by the administration are described *infra* Part III.A.

25. *See* Risen & Lichtblau, *supra* note 23 (noting the White House's stated goals to disrupt terrorist plots and the secrecy with which the executive branch executed the new intelligence-gathering strategy); Letter from William E. Moschella to Pat Roberts et al., *supra* note 24, at 1.

26. *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (allowing the expansion of FISA procedures).

27. *See* Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 26–28 (2005) (outlining the emergence of the prevention strategy). For more on the growth of the FISA court docket see *infra* Part III.C.

central premise of the FISA compromise—authorizing secret electronic surveillance for the purpose of collecting foreign intelligence, but subjecting applications to judicial scrutiny and the entire process to congressional oversight[28]—has been lost.

The change in the purpose requirement and dismantling of the procedural wall in 2002 all but eliminated the protection against skirting Fourth Amendment requirements when misusing FISA to develop evidence for prosecution.[29] FISA became something that it was never intended to be—an alternative to the traditional law enforcement procedures for building a criminal case against alleged terrorists that circumvents constitutional requirements.[30] The TSP is, in some ways, even worse. Unless the executive branch has the constitutional authority to go around FISA, the TSP is a stark violation of limits on surveillance set by Congress.[31] Instead of taking steps to reign in the NSA program, however, Congress is poised either to authorize open-ended and untargeted surveillance programs, or simply to make the FISA procedures optional.[32] Even if Congress takes no action to authorize or regulate the TSP, it will be acquiescing in electronic surveillance activities that lack statutory authority.[33]

Part I reviews the origins of FISA, the modern problems that demand secret surveillance capabilities, and the constitutional and political backdrop for the legislation. It also briefly sets out the statutory provisions and its structure. Part II examines the practice under FISA before September 11, particularly the developments that led to the erection of the wall between law enforcement and foreign intelligence. Part III reviews post-September 11 changes, focusing on the change in the Patriot Act that led to the dismantling of the requirement

28. 18 U.S.C. § 2511(2)(f) (2000 & Supp. III 2003) (stating that FISA is the "exclusive means" to conduct electronic surveillance); Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1809 (2000 & Supp. II 2002) (establishing that it is a criminal offense to conduct electronic surveillance "except as authorized by statute").

29. *See* Banks, *supra* note 16, at 1174–84.

30. *See id.*

31. *See* Risen & Lichtblau, *supra* note 23 (describing the Bush administration's circumvention of established, statutory-derived surveillance procedures).

32. Part. IV.C. discuses the congressional response to the NSA program.

33. See WILLIAM C. BANKS & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW AND THE POWER OF THE PURSE 115–17 (1994) and William N. Eskridge, Jr., *Interpreting Legislative Inaction*, 87 MICH. L. REV. 67, 73–74 (1988) for the legal effects of congressional acquiescence to executive practices.

that "the purpose" of FISA-ordered surveillance be pursuit of foreign intelligence and the avoidance of FISA through the NSA TSP. These two developments lead inexorably to the unraveling of the 1978 FISA compromise and, thus, to the death of FISA. Part IV considers whether technological change makes FISA obsolete, and offers some tentative conclusions on the lawfulness of the TSP. Then I review some proposals to amend and perhaps save FISA while accommodating the TSP, although the prominent efforts in the administration and Congress to amend FISA to accommodate the NSA program and to make optional the use of FISA processes only make more likely the final days of FISA.

I. THE ORIGINS OF FISA

Since our founding as a nation, the government has worried about espionage committed by hostile foreign agents.[34] More recently, the fear of terrorist attacks directed at the United States at home and abroad has overtaken foreign espionage as the preeminent national security threat.[35] To counter these threats, we have relied on many of the techniques used in everyday criminal investigations in pursuit of foreign intelligence, including electronic surveillance, physical searches, and the use of undercover agents and informants.[36] With the digital revolution, communications and surveillance technologies have grown explosively. The government can now watch and listen to telephone, e-mail, or Internet communication in almost any circumstance, and it can power through massive amounts of electronic data in search of relevant information almost instantaneously.[37] The digital revolution does not enable government to collate or assess the importance of the enormous quantity of raw data, leaving that task constrained by human capacities and resources. Even though the amount of collected data that can be evaluated is a small percentage of what is collected, the available intelligence still dwarfs the pre-digital amount.[38]

34. *See* Banks & Bowman, *supra* note 1, at 10–17.

35. *See* THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 43–46 (2006), *available at* http://www.whitehouse.gov/nsc/nss/2006 (discussing the transformation of the objections of national security institutions).

36. Banks, *supra* note 16, at 1151–52.

37. PATRICK J. MCMAHON, CONFERENCE RAPPORTEUR, COUNTERTERRORISM TECHNOLOGY AND PRIVACY 39–55 (2005).

38. *See* PATRICK RADDEN KEEFE, CHATTER: DISPATCHES FROM THE SE-

Now that terrorism has overtaken espionage as the dominant investigative concern in protecting the national security, we have come to realize that terrorism presents difficult challenges in our legal culture. Experience has shown that our criminal laws and traditional law enforcement methods cannot provide sufficient protection against terrorism.[39] Arrest and prosecution have proven successful in some instances, sometimes before and at other times after the planned terrorist act,[40] but the risk that grave harm may occur from a terrorist attack—another September 11, for example, or a biological weapons attack—forces us to look for other preventive tools. Over time, these investigative techniques have anticipated and prevented many plots that would have harmed Americans.[41] Consider these examples:

In 1982, as part of an ongoing investigation of Armenian terrorist groups, FBI agents in Los Angeles monitored a court-authorized electronic surveillance of a home in Santa Monica, trying to learn more about a suspected plot by an Armenian group to bomb the Honorary Turkish Consulate in Philadelphia.[42] During the course of the surveillance, the FBI learned that the targets of the surveillance were building a bomb.[43] Although the plotters managed to transport dynamite inside checked luggage on board a United States commercial airliner, the suspects were arrested before the bomb was moved to its intended target.[44] Criminal convictions were obtained, and the evidence at trial included tape recordings and logs of the electronic surveillance that had been undertaken for the purpose of obtaining foreign intelligence.[45]

In 1981, U.S. citizens affiliated with the Provisional Irish Republican Army (PIRA) sought out a seller of surveillance and

---

CRET WORLD OF GLOBAL EAVESDROPPING 123–25 (2005) (describing the role of human intervention in prioritizing the evaluation of raw intelligence data).

39. *See* Banks & Bowman, *supra* note 1, at 8–10 (noting that the goal of national security—to prevent criminal activity before it occurs—is difficult to reconcile with criminal law legal standards).

40. *See* Chesney, *supra* note 27, at 26–47.

41. *Hearing on U.S. Federal Efforts to Combat Terrorism Before the S. Comm. on Appropriations Subcomm. on Commerce, Justice, State, the Judiciary, and Related Agencies*, 107th Cong. (2001) (statement of John Ashcroft, U.S. Att'y Gen.), *available at* http://www.usdoj.gov/archive/ag/testimony/2001/ag_statement_05_09_01.htm.

42. United States v. Sarkissian, 841 F.2d 959, 961 (9th Cir. 1988).

43. *Id.*

44. *Id.* at 962.

45. *Id.* at 962, 964–65.

counter surveillance equipment, identified themselves as members of the PIRA, and explained that they wanted to use the equipment they would purchase against the British in Northern Ireland.[46] The merchant informed the FBI of this and subsequent conversations, and the FBI began to conduct electronic surveillance of the home telephone of one of the PIRA members.[47] Over time, the surveillance revealed efforts by the target and others affiliated with the PIRA to obtain weapons, including surface-to-air (SAM) missiles.[48] Before their deals were consummated, four PIRA members were arrested and convicted of conspiracy and weapons-related charges, based in part on the fruits of the electronic surveillance.[49]

In 1992, Immigration and Naturalization Service (INS) detained Mohammed Hammoud, a citizen of Lebanon, when he attempted to enter the United States using fraudulent documents.[50] While his application for asylum was pending, Hammoud earned permanent resident status by marrying a United States citizen.[51] In the mid-1990s, Hammoud, along with his wife, a brother, and his cousins became involved in cigarette smuggling.[52] During the same period, Hammoud began leading weekly prayer services for Shi'a Muslims in the Charlotte, North Carolina area, where he urged attendees to donate money to Hezbollah, an organization founded by Lebanese Shi'a Muslims that provides humanitarian aid to Shi'a Muslims and supports terrorism in opposition to Israel and to the United States presence in the Middle East.[53] Hammoud was charged and convicted of providing material support to a designated foreign terrorist organization, along with collateral crimes, including money laundering, credit card fraud, and transportation of contraband cigarettes, in part based on evidence from recorded telephone conversations between Hammoud and others.[54]

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

47. *Id.* at 65–66.

48. *Id.* at 66.

49. *Id.* at 67.

50. United States v. Hammoud, 381 F.3d 316, 325 (4th Cir. 2004) (en banc), *vacated*, 543 U.S. 1097 (2005).

51. *Id.*

52. *Id.*

53. *Id.* at 326.

54. *Id.* at 326–27.

From December 2001 until August 2003, Hemant Lakhani met several times in person and had telephone conversations with an FBI informant who posed as an arms dealer.[55] In 2005, a New Jersey federal jury convicted Hemant Lakhani, an Indian-born United Kingdom national, for attempting to provide material support to terrorists and for his role in trying to sell an anti-aircraft missile to a man whom he believed represented a terrorist group intent on shooting down a United States commercial airliner.[56] Recordings of the conversations and meetings became part of the evidence in the criminal case against Lakhani.[57]

At its most effective, electronic surveillance captures conversations and movements about plans to commit a terrorist act and thus allows the government to step in before the crime occurs. Of course, electronic surveillance may also impose a heavy cost. An array of personal privacy and expressive freedom interests are threatened by electronic surveillance, especially surveillance that is undertaken on a long-term, 24/7 basis.[58] Those who know or suspect the government of monitoring their conversations self-censor their conversations, inhibiting free-flowing expression.[59] Individual interests in anonymity are compromised, as are self-determination choices and freedom of association.[60] As the Supreme Court has noted, electronic surveillance for national security purposes may also implicate a "convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime," when it targets those whose activities are politically motivated.[61] Government interests may be stronger in these areas, but there is also a greater risk of jeopardizing protected expression.[62]

The use of traditional law enforcement techniques brings along with it traditional Fourth Amendment requirements, including the need to establish that a crime has been committed

55. Complaint at 1, United States v. Lakhani, Mag. No. 03-7106 (D.N.J. 2003); *This American Life: The Arms Trader*, *Episode 292* (WBEZ Chicago television broadcast July 8, 2005), *available at* http://www.thislife.org/pages/descriptions/05/292.html.

56. *This American Life: The Arms Trader*, *supra* note 55.

57. Complaint, *supra* note 55, at 1–8.

58. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491–99 (2006).

59. *Id.* at 495.

60. *See id.* at 491–99.

61. United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972).

62. *Id.*

or is imminent before a judge will issue a warrant to conduct electronic surveillance.[63] Because of the gravity of the threat of terrorism and the consequences of those acts, the government has sought the authority to undertake surveillance with something less than the criminal law standard.[64] The grave danger of international terrorism arguably justifies the more permissive FISA regime, and the privacy intrusions are limited to the collection of information for foreign intelligence purposes. At the same time, foreign intelligence collection tends to be programmatic, focusing on nascent schemes and following up on ambiguous leads.[65] In addition, terrorists in a loosely defined cell structure are hard to identify in general, and they are typically trained not to engage in criminal conduct that would justify the criminal variant of electronic surveillance.[66] Ordinary crimes electronic surveillance requires that an application for a warrant contain detailed information about the alleged criminal offense, the facilities and communication sought to be intercepted, the identity of the target (if known), the period of time sought for the surveillance, and an explanation of whether other investigative methods could achieve the objective.[67]

The need for secrecy and the often more open-ended purpose of monitoring a target for foreign intelligence makes the ordinary crimes warrant procedures ill-suited for foreign intelligence gathering.[68] Clearly, something less than a completed act of international terrorism should be required before launching electronic surveillance in pursuit of foreign intelligence.[69] However, deciding just how much evidence of a connection of a potential target to a terrorist group or to terrorist activities should be required is a nettlesome problem.[70] Without suffi-

63. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520 (2000 & Supp. II 2002).

64. Banks & Bowman, *supra* note 1, at 8–10 (discussing the differences in the legal standards for surveillance of terrorism and ordinary crimes investigations).

65. *See* Banks, *supra* note 16, at 1148 (discussing new legislative tools to facilitate intelligence-gathering and analysis).

66. *See* Robert M. Chesney, *Beyond Conspiracy? Anticipatory Prosecution and the Challenge of Unaffiliated Terrorism*, 80 S. CAL. L. REV. 425, 427–28 (2007) (describing the challenges of dealing with unaffiliated terrorists).

67. 18 U.S.C. § 2518(1)(b)–(d) (2000).

68. *See* Banks & Bowman, *supra* note 1, at 5–10.

69. *Id.* at 7, 9 (noting that national security investigations are based on different probable cause standards than criminal investigations as a result of their unique objectives).

70. *Id.* at 5–10.

cient controls, electronic surveillance is an especially ominous form of investigation because, in a digital world, it records and may store and retrieve forever not just the information that investigators seek but everything that the target communicates, no matter how unrelated to the purpose of the surveillance.[71]

The metaphor commonly associated with electronic surveillance is the net that captures everything.[72] If not leavened with controls, electronic surveillance may become the contemporary equivalent of the eighteenth century English general warrants.

The general warrant was abandoned in England, but English law did not recognize a right of privacy.[73] As similar overreaching by Crown agents persisted in the colonies through the use of writs of assistance, colonists lacked a legal remedy.[74] It was thus hardly a surprise that the Bill of Rights would include in the Fourth Amendment protection against the abuses of general warrants.[75]

Of course the Framers could not foresee the problems that would arise in adapting the Fourth Amendment to electronic surveillance. How should its two clauses—the protection against "unreasonable searches and seizures"[76] and the warrant requirement[77]—apply to electronic surveillance? Must pursuit of foreign intelligence follow the Fourth Amendment rules at all, if undertaken inside the United States? If the Fourth Amendment does not offer clear guidance, may Congress legislate to implement and clarify its requirements for gathering information about international terrorism?

Applied to the gathering of foreign intelligence, electronic surveillance offers these same advantages of being able to watch and listen without limitation and to learn about espionage or terrorist activities that may be only in the planning stages. As electronic surveillance became a common tool of law enforcement, so did it enter the world of intelligence investigations in the United States, first by the FBI and then later by

71. Solove, *supra* note 58, at 491–99.

72. *Id.* at 495 (noting that electronic surveillance also records behavior and social interaction).

73. Banks & Bowman, *supra* note 1, at 3.

74. *See* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 29–30 (1970).

75. U.S. CONST. amend. IV.

76. *Id.*

77. *Id.*

the CIA and other intelligence agencies.[78] As countering terrorism became a central national security challenge, the investigative community was faced with the reality that its purpose in investigating might simultaneously be gathering foreign intelligence and enforcing the criminal laws.[79] While the rules for the two types of investigation look very much alike, they differ in some important respects, and they historically remained separate from one another, to protect the integrity of each one.[80]

Only in 1967 did the Supreme Court hold that the Fourth Amendment warrant clause applies to electronic surveillance.[81] In *Katz v. United States*, the Court also held that warrantless searches "are *per se* unreasonable . . . subject only to a few specifically established and well-delineated exceptions."[82] At the time, no foreign intelligence or national security exception had been so recognized, although the *Katz* Court expressly declined to extend its holding to cases "involving the national security."[83] In 1968, Congress responded to *Katz* and enacted legislation creating procedures for judicial authorization of electronic surveillance in law enforcement investigations,[84] but the legislation explicitly noted that Congress did not intend to set rules for national security investigations.[85]

In 1972, the Supreme Court addressed electronic surveillance in a national security setting for the first time. In *United States v. United States District Court* (*Keith*),[86] defendants charged with conspiring to bomb a CIA office in Ann Arbor, Michigan, sought in pretrial proceedings electronic surveillance logs that the government had obtained without a warrant.[87] The government admitted that a warrantless wiretap had in-

78. Banks & Bowman, *supra* note 1, at 19–31.

79. *See, e.g.*, *id.* at 9 (noting that terrorism is the exception to the general rule).

80. *Id.* at 8–9.

81. Katz v. United States, 389 U.S. 347, 353 (1967), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-351, 82 Stat. 212, *as recognized in* United States v. Koyomejian, 946 F.2d 1450, 1455 (9th Cir. 1992).

82. *Id.* at 358.

83. *Id.* at 358 n.23.

84. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2520 (2000)).

85. § 802, 82 Stat. at 214 (repealed 1978).

86. 407 U.S. 297 (1972). This case is typically known as the *Keith* decision, after Damon Keith, the district court judge who presided over the case.

87. *Id.* at 299–300.

tercepted conversations involving the defendants,[88] but it defended the wiretap on the basis of the Constitution and a disclaimer in the 1968 Crime Control Act.[89]

The Court first rejected the statutory argument.[90] The government argued that the provision of the 1968 Crime Control Act regulating electronic surveillance for domestic law enforcement purposes that excluded from its coverage surveillance carried out pursuant to the "constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack . . . [and] to obtain foreign intelligence information deemed essential to the security of the United States"[91] expressed an intention to allow unmonitored electronic surveillance for national security purposes.[92] According to the Court, the disclaimer conferred no new authority and simply left presidential powers untouched.[93]

The Court found authority in the oath clause[94] for the power "to protect our Government against those who would subvert or overthrow it by unlawful means."[95] However, the Court determined that the President must exercise the Article II authority consistently with the Bill of Rights.[96] Although the Attorney General had personally approved the wiretaps and claimed that he had exercised the President's powers to protect the nation against the threat that domestic organizations would attack the government,[97] the Court held that domestic national security wiretaps required a warrant issued by a neutral magistrate.[98] The Court relied on the "broader spirit" of the Fourth Amendment and found that the "convergence of First and Fourth Amendment values" justified special wariness when the government undertakes national security wiretapping.[99] In arriving at its holding, the Court balanced "the duty of Government to protect the domestic security, [against] the

88. *Id.* at 300.

89. § 802, 82 Stat. at 214; *Keith*, 407 U.S. at 302–03.

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

91. § 802, 82 Stat. at 214. The *Keith* Court interpreted the provision as having "left presidential powers where it found them." 407 U.S. at 303.

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

93. *Id.* at 308.

94. U.S. CONST. art. II, § 1.

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

96. *Id.* at 312–13.

97. *Id.* at 300–01.

98. *Id.* at 323–24.

99. *Id.* at 313.

potential danger posed by unreasonable surveillance to individual privacy and free expression."[100] Writing for the Court, Justice Powell concluded that waiving the Fourth Amendment probable cause requirement and allowing "unreviewed executive discretion" to be practiced could cause the executive to "yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[101]

Although the government cited the unique characteristics of ongoing national security surveillance and its fear that leaks could undermine the sources and methods of intelligence collection, the Court refused to recognize an exception to *Katz* for national security surveillance.[102] The Court took note of the potential for abuse of warrantless surveillance, and it noted that courts had the capacity to manage sensitive information and could protect intelligence sources and methods through ex parte proceedings.[103] At the same time, Justice Powell emphasized that the case involved domestic targets of surveillance and that the Court expressed no opinion on the executive discretion to conduct such surveillance when foreign powers or their agents are targeted.[104] In addition, the Court expressly reserved the question whether similar rules should govern foreign intelligence surveillance and, after noting the "different policy and practical considerations from the surveillance of 'ordinary crime'"[105] in investigating national security, the Court supplied a back-handed invitation for Congress to legislate a set of rules for what remained an uncertain terrain—national security investigations—for domestic and foreign intelligence.[106]

Meanwhile, after *Keith*, two courts of appeals upheld the constitutional authorities of the executive branch to conduct warrantless electronic surveillance in pursuit of foreign intelligence.[107] However, the Court of Appeals for the District of Columbiaalso decided a high-profile case at the edges of the post-Watergate prosecution of the White House-ordered break-in of

100. *Id.* at 314–15.
101. *Id.* at 317.
102. *Id.* at 320–21.
103. *Id.*
104. *Id.* at 321–22.
105. *Id.* at 322.
106. *Id.* at 322–23.
107. United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc); United States v. Brown, 484 F.2d 418, 426–27 (5th Cir. 1973).

the Democratic Party headquarters. In *United States v. Ehrlichman*,[108] "Ehrlichman, the former Chief of Staff to President Nixon, argued that the activity he had authorized was a national security, counterintelligence operation, and therefore not illegal."[109] Although the court held that Ehrlichman could not rely on such a defense because he "could not show presidential authorization . . . two of the three judges wrote a separate concurrence [to say that] no intelligence or counterintelligence exception to the Fourth Amendment existed."[110]

FISA was the product of a set of compromises unique to their time. The executive branch wanted a continuing discretion to employ wiretapping for foreign intelligence unfettered by judicial or congressional oversight.[111] Because *Keith* was a domestic security case, the door was not shut.[112] In addition, because *Keith* acknowledged a possibility that the rules might be different for foreign intelligence and the 1968 Crime Control Act disclaimed prescribing any rule for foreign intelligence gathering, it remained plausible to argue that the executive might make its own rules for collecting foreign intelligence.[113] The executive branch's position was weakened considerably, however, by the effects of the Watergate scandal, lawsuits challenging warrantless surveillance, and the practical problem that telephone companies and government agencies were unwilling to approve electronic surveillance without a court order.[114] There were, in addition, high profile investigations of illegal spying by intelligence agencies, including by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the Church Committee).[115] The Church Committee reviewed nearly forty years of domestic

108. 546 F.2d 910 (D.C. Cir. 1976).

109. Diane Carraway Piette & Jessely Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 448 (2006).

110. *Id.*

111. Banks & Bowman, *supra* note 1, at 75.

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

113. *See* Banks & Bowman, *supra* note 1, at 50–52.

114. Piette & Radack, *supra* note 109, at 448; *see also S.2726 to Amend the National Security Act of 1947 to Improve U.S. Counterintelligence Measures: Hearing Before the Select Comm. on Intelligence of the United States S.*, 101st Cong. 136 (1990) (testimony of Mary Lawton, Counsel, Office of Intelligence Policy and Review, U.S. Department of Justice) ("Electronic surveillance can only be done with phone company cooperation . . . .").

115. *See* S. Res. 21, 94th Cong. (1975) (enacted) (describing the investigative committees that reviewed intelligence activities).

surveillance, learning that every President since Franklin D. Roosevelt had asserted and used the authority to authorize warrantless electronic surveillance and finding that "[t]oo many people have been spied upon by too many Government agencies and . . . . Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power."[116] The Church Committee recommended a strict and careful separation of domestic and foreign intelligence gathering, although it recommended continued surveillance of "hostile foreign intelligence activity."[117] The committee summarized the effects of these intelligence abuses in a 1976 report:

> FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate, since typically, each domestic intelligence file contains information on more than one individual or group, and this information is readily retrievable through the FBI General Name Index.
>
> The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics:
>
> - Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953–1973, producing a CIA computerized index of nearly one and one-half million names.
> - At least 130,000 first class letters were opened and photographed by the FBI between 1940–1966 in eight U.S. cities.
> - Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA's Operation CHAOS (1967–1973).
> - Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.
> - An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid-1960's and 1971.

116. 2 SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 5 (1976).

117. *Id.*

- Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.
- At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a "national emergency."[118]

The Committee elaborated:

> Since the 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of a judicial warrant. . . . The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment Rights of both the targets and those with whom the targets communicated. The inherently intrusive nature of electronic surveillance, moreover, has enabled the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens. . . . Also formidable . . . is the 'chilling effect' which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets.[119]

Watergate, the Church Committee and other investigative reports emboldened Congress to control executive overreaching in its use of surveillance. According to the Senate Judiciary Committee, the bill that became FISA was "designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it," but to authorize the use of electronic surveillance to obtain foreign intelligence information.[120] Civil liberties groups, such as the ACLU, worried that if Congress set a wiretap standard too low, it could end up "authorizing rather than curtailing intelligence agency abuses."[121] In other words, would no legislation be better for

118. *Id.* at 6–7.

119. S. REP. NO. 95-604, at 8 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3909.

120. *Id.* at 8–9.

121. *See Foreign Intelligence Surveillance Act of 1977: Hearing on H.R. 5794, H.R. 9745, H.R. 7308, H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 92 (1978) (statement of John H.F. Shattuck, Executive Director, ACLU, Wash. Office), *available at* http://www.cnss.org/fisa011078.pdf [hereinafter *FISA Hearing*]; *see also* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 808–11 (1989) (discussing the compromises made between

civil liberties than bad legislation? At the same time, Congress recognized that "no persons should be targeted for electronic surveillance unless the Government has evidence they are engaging in criminal conduct which directly threatens national security,"[122] even though evidence of national security crimes could be collected during the electronic surveillance. While this suspicion of criminal activity was an essential part of what would become the FISA provisions that apply to United States citizens, Congress did not intend for FISA to authorize surveillance for the purpose of enforcing the criminal laws.[123] Congress understood that intelligence gathering and law enforcement would overlap, and that congressional oversight could monitor the uses of FISA-ordered evidence in criminal prosecutions.[124]

After six years of hearings and discussion and through the stewardship of Attorneys General Edward Levi and Griffin Bell, Presidents Gerald Ford and Jimmy Carter, and several members of the House and Senate, FISA became law in 1978.[125] In his signing statement, President Carter said:

> The bill requires, for the first time, a prior judicial warrant for *all* electronic surveillance for foreign intelligence or counterintelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign intelligence by electronic surveillance in the United States. It will remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism. It will assure FBI field agents and others involved in intelligence collection that their acts are authorized by statute and, if a U.S. person's communications are concerned, by a court order. And it will protect the privacy of the American people.
>
> In short, the act helps to solidify the relationship of trust between the American people and their Government. It provides a basis for the trust of the American people in the fact that the activities of their intelligence agencies are both effective and lawful. It provides enough secrecy to ensure that intelligence relating to national security can be securely acquired, while permitting review by the courts and Congress to safeguard the rights of Americans and others.[126]

proponents and opponents of national security electronic surveillance legislation).

122. *FISA Hearing*, *supra* note 121, at 92.

123. *See* Banks, *supra* note 16, at 1160.

124. SENATE SELECT COMM. ON INTELLIGENCE, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. REP. NO. 98-660, at 14 (1984).

125. *Id.* at 1.

126. JIMMY CARTER, STATEMENT ON SIGNING S. 1566 INTO LAW 1853–54

FISA's authorization of electronic surveillance of "foreign powers" and their agents, terms taken from the Supreme Court in *Keith* reflects the Act's focus on foreign intelligence.[127] From the beginning, the definition of "foreign power" has included "a group engaged in international terrorism or activities in preparation therefor."[128] An "agent of a foreign power" included a person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power."[129] The term "foreign intelligence information" was defined as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[130]

Non-United States persons (someone not a citizen or permanent resident, among others) could be an "agent of a foreign power" by being an officer or employee of a foreign power, or a member of an international terrorist organization.[131] The government could target United States persons as agents only if they knowingly engaged in certain activities, including international terrorism which "involve or may involve a violation of the criminal statutes of the United States."[132]

The FISA process authorizes "electronic surveillance," which is broadly defined and must fall within one of four categories:

> (1) the acquisition by an electronic, mechanical, or other surveil-

(1978), http://www.cnss.org/Carter.pdf.

127. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308, 321–22 (1972).

128. 50 U.S.C. § 1801(a)(4) (2000).

129. *Id.* § 1801(b)(2)(C).

130. *Id.* § 1801(e).

131. *Id.* § 1801(b)(1)(A).

132. *Id.* § 1801(b)(2)(A).

> lance 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, mechanical, or other surveillance 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, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance 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; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[133]

The definition excludes electronic surveillance of communications taking place entirely abroad, but it reaches wire or radio communications sent by or intended to be received by a targeted United States person, and those to or from any person within the United States without the consent of one party, where the interception occurs inside the United States.[134] In the event of a question concerning whether FISA applies to a particular form or use of electronic surveillance, the Senate Judiciary Committee stated in 1977 that "this statute, not any claimed presidential power, controls."[135]

In return for subjecting the executive branch to regulation of its electronic surveillance activities, FISA does not provide the traditional protections against government abuse of its electronic surveillance in enforcing the criminal laws.[136] FISA

133. *Id.* § 1801(f).

134. *Id.* § 1801(f)(1)–(2).

135. S. REP. NO. 95-604, at 64 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3965. The House Conference Report noted that the "exclusive" provision "does not foreclose a different decision by the Supreme Court." H.R. REP. NO. 95-1720, at 35 (1978) (Conf. Rep.), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4064.

136. For example, targets of law enforcement surveillance must be given notice of the surveillance within ninety days of its termination. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat.

put in place a much more government-friendly process. Instead of a neutral magistrate finding probable cause to believe that a particular crime has been, is being, or is about to be committed and then issuing a warrant that is later noticed to the target,[137] FISA authorizes a special court, the Foreign Intelligence Surveillance Court (FISC), that meets in secret, ex parte.[138] To permit electronic surveillance without the target ever learning that she was a target, based on a showing that pursuit of foreign intelligence is a significant purpose of the surveillance, and that there is probable cause to believe that the target is a foreign power or agent of a foreign power.[139]

The target may eventually learn of the FISA targeting only if the FISA surveillance is used by the government in a criminal or other proceeding against him before its use against the target.[140] Only the judge reviewing the lawfulness of the surveillance sees the surveillance logs, in camera.[141] Applications to the FISC must pass through layers of review inside the Justice Department and obtain the approval of the Attorney General.[142] The order must describe in some detail the targets of

197 (codified as amended at 18 U.S.C. §§ 2510–2520 (2000)). Criminal defendants routinely obtain access to the application for surveillance, supporting affidavits, surveillance logs, and statements from informants. 18 U.S.C. § 2518(9).

137. 18 U.S.C. § 2518.

138. 50 U.S.C. § 1803(a) (2000).

139. The FISC grew from seven to eleven judges with enactment of the Patriot Act. *See* Patriot Act, Pub. L. No. 107-56, § 208, 115 Stat. 272, 283 (2001) (codified as amended at 50 U.S.C. § 1803(a)). If the government does not prevail before the FISC, it may appeal to a three-judge FISA Court of Review. 50 U.S.C. § 1803(b) (2000).

140. 50 U.S.C. §§ 1802(a)(3), 1806(f)–(g) (2000). FISC does not publish its decisions, its orders are sealed, proceedings are ex parte. *See id.* § 1806(f).

141. *Id.* § 1806(f). A reviewing court reviews the materials ex parte and in camera and only discloses them to the defendant "where disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* If the Attorney General files a claim of privilege in a pending proceeding against the target of FISA surveillance, the targets of surveillance may not be able to examine materials related to the surveillance. *Id.* A district court may review FISC-ordered surveillance and may overturn a nondisclosure decision if the certifications of compliance with FISA requirements are clearly erroneous. *Id.* No court has ordered disclosure. *Id.*; *see also, e.g.*, ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 469–71 (D.C. Cir. 1991) (explaining why district courts rarely overturn nondisclosure decisions).

142. 50 U.S.C. § 1805(a)(2); *see also* Piette & Radack, *supra* note 109, at 460 ("'[T]he FBI played a much stronger role in reviewing and drafting cases' and . . . 'there were some 25 layers of review at the Bureau before the Director signed off on [an] application and it came back to our office for AG approval . . . .'") (quoting a former Justice department lawyer).

the surveillance and the places where surveillance will occur.[143] Time limits are set for the surveillance, although there are opportunities to extend the time.[144] Also, once the statutory findings are made by the FISC, the judge "shall" issue the surveillance order.[145]

To reduce the chance that FISA surveillance could interfere with the rights of U.S. persons, FISA requires "minimization procedures" that the Attorney General must adopt in order to curtail acquisition and retention and prohibit dissemination of nonpublic information about U.S. persons.[146] In essence, FISA forbids disclosing information obtained from FISA surveillance except as provided in the minimization procedures,[147] although "information that is evidence of a crime which has been, is being, or is about to be committed can be retained or disseminated for law enforcement purposes."[148]

To underscore that Congress intended this new scheme to replace entirely the previously unregulated electronic surveillance practices of the executive branch, federal law includes a provision stating that its procedures, along with those prescribing rules for law enforcement surveillance, provide the "exclusive means" of engaging in electronic surveillance.[149] The provision also clarified that the exclusivity provision does not cover other foreign electronic surveillance conducted abroad, including any such surveillance that targets U.S. persons.[150] Another FISA provision makes it a crime to conduct electronic surveillance "except as authorized by statute."[151]

FISA also includes authorization for surveillance outside the FISA process for up to one year when directed solely at "communications transmitted by means of communications used exclusively between or among foreign powers" and there is "no substantial likelihood" that communication involving a U.S. person will be acquired.[152] However, this is a narrow exception

143. 50 U.S.C.A. § 1805(c)(1) (West 2003 & Supp. 1A 2006).

144. *Id.* § 1805(e).

145. 50 U.S.C. § 1805(a) (2000).

146. *Id.* §§ 1801(h)(1), 1805(a)(4).

147. *Id.* § 1806(a).

148. *Id.* § 1801(h)(3). Problems of minimization and prosecution are considered *infra* notes 515–50 and accompanying text.

149. 18 U.S.C. § 2511(2)(f) (2000 & Supp. III 2003).

150. *Id.*

151. 50 U.S.C. § 1809(a)(1) (2000).

152. *Id.* § 1802(a)(1). The effects of new technology on FISA are addressed *infra* Part IV.A.

to the default FISA processes. Because this exception for programmatic surveillance is allowed only for direct foreign government communications, it does not allow surveillance outside the FISA process when foreign powers use public communications networks. Congress built into law two other exceptions to the exclusivity of the FISA process gathering for foreign intelligence. One section permits surveillance outside FISA for up to fifteen days following a declaration of war,[153] and the other permits the Attorney General to certify that "an emergency situation exists" that requires electronic surveillance before an order from the FISC could be obtained.[154] The emergency authority may be exercised for up to seventy-two hours from the time authorization is made by the Attorney General, until the information sought is obtained, or until the FISC denies the application for surveillance, whichever is earlier.[155] The emergency procedures still demand an application to a judge, but it is not required until seventy-two hours after the emergency authorization.[156]

Although the scheme was complex, the compromise struck a fundamental balance. Those most worried about the abuses of past presidents and their subordinates took comfort in the regulation of foreign intelligence surveillance that involved Article III judges, albeit to a limited extent. The secrecy, *ex parte* proceedings, and corresponding lack of notice to the targets was troubling, but at least the procedures were prescribed by law. From the executive branch and intelligence investigators' perspectives, what was done in the past on the basis of supposed inherent constitutional authority was now subject to rules imposed by Congress, but once learned and followed, the rules lent legitimacy to secret surveillance.

II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT PRACTICE UP TO SEPTEMBER 11

Between 1978 and the early 1990's, FISA operated to the satisfaction of the principally involved institutions, and it changed only incrementally. FISA applications grew in number during this period, although the growth was modest until 1995 (following the first World Trade Center and Oklahoma City

153. 50 U.S.C. § 1811.
154. *Id.* § 1805(f)(1).
155. *Id.* § 1805(f).
156. *Id.*

bombings), when the number of annual orders doubled from the early years, to about one thousand by 2001.[157] The executive branch could hardly complain—it always, or nearly always, got what it wanted when it made an application to the FISC.[158] Inside the Justice Department, the FBI was required to change the way it had always operated, and it did so primarily through the promulgation and implementation of sets of guidelines, first issued by Attorney General Edward Levi in 1976.[159] The FBI guidelines, revised by successive administrations, followed the FISA strictures and supplied more detail for investigations, including those outside the triggering language of FISA.[160] Meanwhile, federal courts upheld FISA against constitutional challenges and supported the use of FISA surveillance as evidence in criminal cases after finding that the "primary purpose" of the surveillance was to gather foreign intelligence.[161]

In addition, the Justice Department created a central gatekeeper for all FISA applications, the Office of Intelligence Policy and Review (OIPR). OIPR was assigned to represent the United States before the FISC and to ensure institutional responsibility for FISA compliance,[162] allowing FISA expertise to

157. Until expanded reporting requirements were required beginning in 2005, brief annual reports of FISA activity were provided by the Attorney General, including the volume of applications approved for the year. *See* Foreign Intelligence Surveillance Act, http://www.fas.org/irp/agency/doj/fisa (follow "FISA Annual Reports to Congress" hyperlink) (last visited Apr. 13, 2007). The reports show an average of five hundred to six hundred requests in the 1980s and early 1990s before an increase after 1995. *See id.* The more recent reporting requirements are addressed *infra* 325–327.

158. After more than twenty years, only two FISA applications had been rejected. In 1981, the FISC ruled that it had no jurisdiction to approve an application for a physical search for national security purposes. *In re the Application of the U.S. for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property* (F.I.S.C. 1981), *as reprinted in* S. REP. NO. 97-280, at 16–19 (1981). In 1997, an application for electronic surveillance was rejected "with leave to amend," but the government did not pursue the matter. *Supreme Court Rebuffs FISA Challenge*, SECRECY NEWS, Apr. 23, 2001, *available at* http://www.fas.org/sgp/news/secrecy/2001/04/042301.html.

159. STAFF OF THE SUBCOMM. ON SEC. AND TERRORISM OF THE SENATE COMM. ON THE JUDICIARY, 97th CONG., THE DOMESTIC SECURITY INVESTIGATION GUIDELINES 51–64 (Comm. Print 1982) [hereinafter DOMESTIC SECURITY GUIDELINES]. For a review of these and subsequent versions of the guidelines, see STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 617–27 (4th ed. 2007).

160. *See* DOMESTIC SECURITY GUIDELINES, *supra* note 159.

161. *See, e.g.*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Rahman, 861 F. Supp. 247, 251 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999).

162. *See* Office of Intelligence Policy and Review, http://www.fas.org/irp/

develop inside the Department. Their office sought to make FISA applications detailed and complete.[163] When OIPR delivered applications to the FISC, the Department could represent that it sought electronic surveillance in pursuit of a "foreign intelligence" purpose, not to spy on political enemies or to end-run the magistrate in building a criminal case.[164]

As the federal courts admitted FISA-obtained evidence in criminal prosecutions after finding that the primary purpose of the investigation was to collect foreign intelligence, OIPR performed its gatekeeping role to assure that the Department of Justice followed FISA procedures. Under OIPR head Mary Lawton, who ran OIPR from 1982 until her sudden death in 1993, OIPR operated without written guidelines.[165] Although Lawton believed that some things were better "left undefined," she and OIPR made sure that the intelligence and law enforcement personnel regularly consulted one another.[166] The 9/11 Commission Report and an Inspector General's report on the FBI and intelligence related to the September 11 attacks concluded that, from the inception of FISA through the early 1990's, "prosecutors had informal arrangements for obtaining information gathered in the FISA process,"[167] and that "prosecutors within the Department's Criminal Division . . . had to be consulted in connection with intelligence investigations in which federal criminal activity was uncovered, or when legal advice was needed to avoid investigative steps that might inadvertently jeopardize the option of prosecution using information obtained from the intelligence investigation."[168]

Gradually, the insistence of OIPR and the FISC on fulsome FISA applications resulted in more elaborate procedures, including those that separated law enforcement and intelligence agents and activities.[169] Although implementation of the FISA purpose requirement was to some extent responsible for devel-

agency/doj/oipr/index.html (last visited Apr. 13, 2007).

163. *See* Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance,* 17 STAN. L. & POL'Y REV. 531, 535 (2006).

164. *Id.*

165. *See* Piette & Radack, *supra* note 109, at 449–52.

166. *Id.* at 451–52.

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

168. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 24 (2004) [hereinafter 2004 OIG REPORT].

169. *Id.* at 25–27.

oping what evolved into a "wall," to a large degree the barriers between successful intelligence and law enforcement cooperation and sharing were due to a perennially cumbersome FBI bureaucracy, an equally bad FBI computer system, and a culture inside the Criminal Division and intelligence sides of the FBI that simply nurtured separation.[170]

For several years, the OIPR role in managing the FISA process evolved without major incidents.[171] However, during the Aldrich Ames espionage prosecution in 1994, back-channel cooperation between the CIA and FBI prompted OIPR to advise the Attorney General that the close CIA/FBI collaboration in the Ames investigation could provide Ames' lawyers with an argument that the FISA warrants were misused.[172] Ames accepted a plea bargain, so no test of the OIPR concern was presented to a judge.[173] Still, the Justice Department was put on notice that back-channel consultations between its intelligence and law enforcement officials could be problematic.

Inside the Justice Department, Deputy Attorney General Jamie Gorelick convened a working group to reconcile emerging differences of opinion between OIPR, the Criminal Division, and FBI over "wall" issues.[174] The working group sought an opinion from the Office of Legal Counsel (OLC) on the question of whether the FISC could approve a search under FISA only when the collection of foreign intelligence was the "primary purpose" of the search, or whether it sufficed that such collection was one of the purposes.[175] In February 1995, the OLC "concluded that '"courts are more likely to adopt the 'primary purpose' test than any less stringent formulation."'"[176] Based on

170. Schulhofer, *supra* note 163, at 535–36 ("FISA's 'purpose' requirement was a seed from which increasingly intricate obstacles developed. Yet the resulting problems were not inevitable, even under the law as it stood before 9/11; most of the difficulties could have been avoided with better training, more common sense, and more willingness to tolerate ambiguity and decentralized discretion.").

171. *See* 9/11 COMMISSION REPORT, *supra* note 167, at 78.

172. *Id.*

173. STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 665 (2d ed. 1997).

174. *See* 9/11 COMMISSION REPORT, *supra* note 167, at 79.

175. *See* U.S. DEP'T OF JUSTICE, FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION 720 (May 2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows.htm [hereinafter BELLOWS REPORT].

176. *Implementation of the USA PATRIOT ACT: Section 218—Foreign Intelligence Information ("The Wall"): Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th

the FISA case law, OLC determined that "the greater the involvement of prosecutors in the planning and execution of FISA searches, the greater is the chance that the government could not assert in good faith that the 'primary purpose' was the collection of foreign intelligence."[177] OLC thus recommended that "an appropriate internal process" should be established "that FISA certifications are consistent with the 'primary purpose' test."[178]

Meanwhile, to assure that misuse of FISA did not occur, OIPR began imposing information-sharing controls on its own initiative.[179] The working group made recommendations to Deputy Attorney General Gorelick, who in turn submitted them to Attorney General Reno.[180] In March 1995,[181] Gorelick wrote a memorandum prescribing special "wall" procedures for two pending cases, including the 1993 World Trade Center bombing prosecution.[182] The memorandum instructed that the intelligence investigation in the New York case would go forward "without any direction or control"[183] by the U.S. Attorney's office or the Criminal Division, and it required FBI headquarters or OIPR approval to share some portions of intelligence investigative memoranda with law enforcement agents.[184] In addition to these "wall" procedures, the March memorandum also encouraged cooperation and coordination between the intelligence and law enforcement personnel in a few particular ways.[185] According to a 2004 Office of the Inspector General report, the March memorandum from Gorelick was somehow misconstrued and its "wall" procedures were applied through-

Cong. 17–34 (2005) (statement of David S. Kris, Senior Vice President, Time Warner Inc.), *available at* http://judiciary.house.gov/media/pdfs/kris042805.pdf.

177. *Id.*

178. *Id.*

179. 9/11 COMMISSION REPORT, *supra* note 167, at 78.

180. *Id.* at 79.

181. *See id.* at 539 n.83 (stating that Jamie Gorelick authored the memo to Mary Jo White in March, 1995).

182. *See* Memorandum from Jamie S. Gorelick, Deputy Attorney Gen., to Mary Jo White, U.S. Attorney, S. Dist. of N.Y., et al. 1–4 (Mar. 1995) [hereinafter Gorelick Memo] (regarding "Instructions on Separation of Certain Counterintelligence and Criminal Investigations"), *available at* http://www.usdoj.gov/ag/testimony/2004/1995_gorelick_memo.pdf.

183. *Id.* at 3.

184. *Id.*

185. *See id.* at 2–3.

out the FBI for all FISA applications by 1997.[186] Notably, the restrictive procedures in the Gorelick memorandum exceeded any requirements imposed by FISA or case law.[187]

Then, in July 1995, Attorney General Janet Reno issued a set of secret internal guidelines to prescribe procedures for contacts among the Justice Department's Criminal Division, the FBI, and OIPR.[188] Contacts between the prosecutors and their investigators and intelligence officials were limited, logged, and noted to the OIPR.[189] These entities could exchange consultations and advice, but the contacts should "not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling" an investigation.[190] The guidelines were not written to affect contacts and information-sharing between investigating agents—internal to the Criminal Division or between criminal and intelligence investigators—but instead were intended to apply only between investigators and prosecutors.[191]

According to a later Office of the Inspector General Report, the OIPR lawyers almost immediately misconstrued and misapplied the 1995 guidelines as containing the special procedures imposed in New York by the March Gorelick memorandum, thus interpreting FISA as essentially prohibiting contact between the law enforcement and intelligence sides of an investigation.[192] Coordination between law enforcement and intelligence officials that had occurred before 1995 fell off after issuance of the guidelines, and such contacts that did occur came so

186. *See* 2004 OIG REPORT, *supra* note 168, at 31.

187. *See* Gorelick Memo, *supra* note 182, at 2 (explaining that the recommended procedures "go beyond what is legally required").

188. *See* Memorandum from Janet Reno, Attorney Gen., to Assistant Attorney Gen., Criminal Div., et al. (July 19, 1995) (regarding "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations"), *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html.

189. *See id.*

190. *Id.* pt. A.6.

191. 9/11 COMMISSION REPORT, *supra* note 167, at 79; *see also* LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11, at 343 (2006) ("The Justice Department promulgated a new policy in 1995 designed to regulate the exchange of information between agents and criminal prosecutors, but not among the agents themselves.").

192. 9/11 COMMISSION REPORT, *supra* note 167, at 79 ("[The] procedures were almost immediately misunderstood and misapplied."); 2004 OIG REPORT, *supra* note 168, at 33; WRIGHT, *supra* note 191, at 343 ("Bureaucratic confusion and inertia allowed the policy to gradually choke off the flow of essential information . . . .").

late in the process as to be practically useless.[193] Although not required by FISA, a metaphorical "wall" between law enforcement and intelligence gathering was thus put in place whenever an intelligence investigation suggested some indication of criminal activity.[194] The FBI then developed a parallel system of "dirty" teams for gathering intelligence and "clean" teams for criminal law enforcement.[195] The teams could investigate the same target at the same time, but they rarely talked with one another.[196]

OIPR maintained its gatekeeper role throughout this period—only through it would information pass to the Criminal Division. According to the 9/11 Commission, OIPR sustained its position in part by maintaining it reflected the concerns of the chief judge of the FISC, and that "if it could not regulate the flow of information to criminal prosecutors, it would no longer present the FBI's warrant requests to the FISA Court."[197] Although the OIPR FISA procedures were revised between 1995 and 2002 to permit consultation between the intelligence and prosecution sides of the FBI "aimed at preserving the option of criminal prosecution," the Criminal Division was not allowed to "*direct or control* the FISA investigation."[198] During this period, the FISC approved the OIPR procedures and issued case-specific information screening walls.[199] These mechanisms varied with the complexity of the investigation, and sometimes saw the FISC serving as the "wall" between the two sides.[200] In 1999, a badly managed espionage investigation of Los Alamos

193. *See Hearing*, *supra* note 15, at 49.

194. *See* WRIGHT, *supra* note 191, at 343 (characterizing the FISC as the "arbiter of what information could be shared—'thrown over the Wall'").

195. Roberto Suro, *FBI's "Clean" Team Follows "Dirty" Work of Intelligence*, WASH. POST, Aug. 16, 1999, at A13.

196. *Id.*; *see also Hearing*, *supra* note 15, at 49–50 (describing the guidelines as leading to decreased coordination on intelligence cases); U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 4 (2001) ("[The] implementation and interpretation of the procedures . . . led to a significant decline in coordination between the FBI and the Criminal Division.").

197. 9/11 COMMISSION REPORT, *supra* note 167, at 79.

198. *In re* Sealed Case, 310 F.3d 717, 729; *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 619 (FISA Ct. 2002), *abrogated by In re Sealed Case*, 310 F.3d 717.

199. 9/11 COMMISSION REPORT, *supra* note 167, at 539 n.83.

200. *See id.*

National Laboratory scientist Wen Ho Lee[201] led the Attorney General to appoint a commission to review the Lee investigation, including the apparent failure to take advantage of FISA procedures.[202] The investigation found that the FBI should have sought and obtained FISA surveillance of Lee, and that OIPR insisted that the Justice Department have more evidence of foreign agency than FISA requires.[203]

III. THE POST-SEPTEMBER 11 CHANGES

The euphemism that "everything changed"[204] after the September 11 attacks probably exaggerates less what happened to FISA than to most other pre-attack authorities in the counter-terrorism area. Critics of the Patriot Act who do not know its lineage often complain that the massive bill and its many controversial amendments to FISA and to other laws was rushed through Congress by the Bush administration and that members only hastily and cursorily reviewed the bill in the seven weeks between its introduction and enactment.[205] Although the rush to judgment in Congress was real, the Justice Department had drafts of portions of what would become the Patriot Act prepared and waiting before the September 11 attacks—the hijackers provided the political atmosphere needed to provide favorable consideration of some significant changes in the law.[206] Still, no committee reports accompanied the Pa-

201. *See* Bob Drogin, *How FBI's Flawed Case Against Lee Unraveled*, L.A. TIMES, Sept. 13, 2000, at 1.

202. *See* BELLOWS REPORT, *supra* note 175, at 14–15.

203. *See id.* at 482–83, 497.

204. *See, e.g.*, Editorial, *"The Day That Everything Changed,"* L.A. TIMES, Sept. 13, 2001, at 8 (stating that September 11 was "the day that everything changed in our country").

205. *See* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1145–46 (2004); *id.* at 1151–52 (noting "the dangers inherent in the haste to legislate" and that on September 17, 2001, Attorney General Ashcroft called for Congress to pass the administration's unseen and not completely drafted bill that week); *see also* Clayton Northouse, *Interview with U.S. Senator Russ Feingold, April 21, 2004*, *in* PROTECTING WHAT MATTERS: TECHNOLOGY, SECURITY AND LIBERTY SINCE 9/11 72, 72–80 (Clayton Northouse ed., 2006) (interviewing Sen. Russ Feingold, the only senator to vote against the Patriot Act).

206. *See* JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR 71 (2006) (stating that career lawyers at the Justice Department developed a "wish list" of proposals for the Patriot Act from provisions not passed when Congress enacted antiterrorism legislation in 1996).

triot Act describing and explaining any fundamental rethinking of the basic terms of the FISA compromise of interests.[207]

Two developments merit special attention because, taken together, they portend the death of FISA—one section of the Patriot Act[208] with its implementation by the FISA Court of Review and the NSA Terrorist Surveillance Program (TSP).

A. THE COLLAPSE OF THE FOREIGN INTELLIGENCE PURPOSE RULE

Until amended by the Patriot Act, FISA required that an application to the FISC for electronic surveillance had to include a certification that "the purpose of the surveillance is to obtain foreign intelligence information."[209] As interpreted by the federal courts between FISA's implementation and 2001, in practice the rule was that the "primary purpose" of the FISA surveillance must be to obtain foreign intelligence.[210] If and when a law enforcement purpose became dominant in an investigation, FISA required that traditional criminal investigative rules be followed in order to continue the surveillance.[211]

In enacting FISA, Congress understood that, in many situations, intelligence and law enforcement investigators work side-by-side and that information collected in intelligence gathering becomes evidence in an eventual criminal proceeding.[212] In the aggregate, however, foreign intelligence gathering is programmatic, rather than targeting specific individuals for known or anticipated crimes.[213] Intelligence investigations often continue long after a completed criminal act has been prosecuted.[214] In addition, the product of foreign intelligence investigations may, at any point in time, appear fragmented

207. *See* Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOK. J. INT'L L. 175, 227 (2003) (stating that no committee reports accompanied the Patriot Act).

208. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 § 218 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)).

209. 50 U.S.C. § 1804(a)(7)(B) (2000) (current version at 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2003)).

210. *See* Banks, *supra* note 16, at 1159.

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

212. Banks & Bowman, *supra* note 1, at 4.

213. *See* Banks, *supra* note 16, at 1152.

214. *Id.*

and hard to evaluate to someone in law enforcement.[215] The culture of criminal investigations, including the legal standards of particularity, criminality, and eventual notice to the target, has no parallel in the world of foreign intelligence gathering.[216]

The intelligence gathering and law enforcement spheres overlapped in 1978, and they overlap to a greater extent now.[217] Intelligence investigations turn up leads that provide the criminal investigators what they need to make a case.[218] The criminal enforcement team may gain intelligence during the course of their surveillance or in an interrogation.[219] However, as counter-terrorism officials recognized the value of collaboration between intelligence and law enforcement investigators, they also confronted formidable institutional—not legal—resistance.[220] The tension between the need for secrecy and the demand to share information is inevitable, long-standing, and entrenched.[221] From the intelligence side, leaks are anathema, and compromised sources have no value.[222] Criminal investigators and prosecutors work assiduously to avoid tainting prosecution evidence through contact with intelligence officials whose knowledge could render critical evidence inadmissible.[223] The law requires the use of law enforcement investigative procedures if the sole purpose of surveillance is prosecution, and it permits FISA procedures if the purpose of the investigation is the collection of foreign intelligence.[224] To some extent, the "wall" procedures grew out of concern for preserving these baseline rules.[225] By and large, however, the separate institutional responsibilities and concerns are reflected in the separate divi-

215. *Id.*

216. *Id.*

217. *See infra* notes 291–95 and accompanying text.

218. *See* Banks & Bowman, *supra* note 1, at 4.

219. 9/11 COMMISSION REPORT, *supra* note 167, at 424.

220. *See id.* at 79 (describing the barriers to information-sharing as the "wall").

221. *See* MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 18 (3d ed. 2006).

222. *See* Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331, 337–38 (1998).

223. *See id.*; WRIGHT, *supra* note 191, at 205 ("[FBI personnel] tended to be close-mouthed and unhelpful, treating all intelligence as potential evidence that couldn't be compromised, whether there was an actual criminal case or not.").

224. *See* 9/11 COMMISSION REPORT, *supra* note 167, at 78.

225. *See id.* at 79 (describing the "wall" as an accumulation of "institutional beliefs and practices").

sions for criminal and national security investigations inside the FBI, and they show that the "wall" is much more grounded in cultural or institutional matters than it is in legal concerns.[226] The institutional differences, rivalries, and bureaucracies transcend the FBI and include the CIA and NSA, before and after September 11.[227]

When the failures in information-sharing and cooperation surrounding the September 11 hijackers came to light,[228] the Bush administration determined to lower the supposed barriers and turn loose all the investigative resources available in a paradigm of prevention[229] to complement prosecution and other means of combating terrorism. Initially, the Justice Department proposed an amendment that would have replaced FISA's certification requirement that "the purpose" of surveillance was to obtain foreign intelligence with "'a' purpose."[230] According to the Department, the change "would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities."[231] Even in the short time given to consider the proposal, members objected that the "a purpose" standard would open the door for virtually unlimited use of FISA in criminal investigations, where foreign intelligence is only remotely connected

226. *See* WRIGHT, *supra* note 191, at 242 ("[T]he two men most responsible for putting a stop to bin Laden and al-Qaeda . . . disliked each other intensely . . . . From the start, the response of American intelligence to the challenge presented by al-Qaeda was hampered by the dismal personal relationships and institutional warfare that these men exemplified.").

227. *Id.* at 283 (stating that after the African embassy bombings, the NSA monitored satellite phone calls of senior al Qaeda leaders, but refused to share the raw data with the FBI, CIA, or White House counter-terrorism officials); *id.* at 312 (noting that the CIA distrusted the senior FBI official and feared that the FBI "was too blundering and indiscriminate to be trusted with sensitive intelligence"); *id.* at 314–15, 340–42 (noting that the CIA knew the 9/11 hijackers in the United States but that the CIA did not share that information with the FBI); *id.* at 343 (suggesting that the CIA and NSA restricted information-sharing after "eagerly institutionaliz[ing]" the "wall").

228. Two of the suspected 9/11 hijackers had been on a CIA watch list, but the CIA informed the FBI only after they entered the United States. Guy Gugliotta, *Terrorism "Watch List" Was No Match for Hijackers*, WASH. POST, Sept. 23, 2001, at A22.

229. U.S. DEP'T OF JUSTICE, FACT SHEET, *supra* note 6.

230. DEP'T OF JUSTICE, ANTI-TERRORISM ACT OF 2001, SECTION-BY-SECTION ANALYSIS (2001), *available at* http://www.eff.org/Censorship/Terrorism_militias/20010919_doj_ata_analysis.html.

231. *Id.*

to the investigation.[232] Even a Justice Department FISA expert admitted that the proposed amendment to the purpose language had less to do with what information could be collected than with facilitating coordination between intelligence and law enforcement after collection.[233] Senator Leahy then proposed a new provision to facilitate information sharing, independent of the purpose certification and the administration agreed to his proposal.[234] The new section was enacted and it permits those who acquire foreign intelligence by conducting electronic surveillance to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" terrorist activities by foreign powers or their agents.[235]

During the course of the Congressional debate, members and outside experts questioned the constitutionality of the change to "a" purpose, from "the" or "primary" purpose.[236] Al-

232. Beryl A. Howell, *Foreign Intelligence Surveillance Act: Has the Solution Become the Problem?*, *in* PROTECTING WHAT MATTERS: TECHNOLOGY, SECURITY, AND LIBERTY SINCE 9/11 118, 124 (Clayton Northouse ed., 2006).

233. *Protecting Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. on the Constitution, Federalism, and Property Rights of the S. Comm. on the Judiciary*, 107th Cong. 65 (2001) [hereinafter *Protecting Constitutional Freedoms*] (testimony of David S. Kris, Assoc. Deputy Att'y Gen.); *see also S. 1448, The Intelligence to Prevent Terrorism Act of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing before the S. Select Comm. on Intelligence*, 107th Cong. 21 (2001) [hereinafter *Intelligence to Prevent Terrorism Act*] (testimony of David S. Kris, Assoc.iate Deputy Att'y Gen.) ("[T]he administration's proposal [is] designed to foster and facilitate greater coordination between the law enforcement and the intelligence sides of the Government.").

234. *See Statement of Senator Patrick Leahy, Chairman, Senate Judiciary Comm., and Democratic Manager of the Senate Debate on the Anti-Terrorism Bill* (Oct. 25, 2001), http://leahy.senate.gov/press/200110/102501.html.

235. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 504(a), 115 Stat. 272, 364–65 (codified at 50 U.S.C. §§ 1806(k), 1825(k)). The Act states that such coordination "shall not preclude" the required FISA certification. *Id.*; *see also* 50 U.S.C. § 1804(a)(7)(B) (2000) (requiring certification that "a significant purpose" of the surveillance requested is to obtain foreign intelligence).

236. *See Protecting Constitutional Freedoms*, *supra* note 233, at 45–46 (statement of Morton Halperin, Senior Fellow, Council on Foreign Relations); *Intelligence to Prevent Terrorism Act*, *supra* note 233, at 44–45 (2001) (prepared statement of Jeffrey H. Smith, Partner, Arnold & Porter) (arguing that the "Committee should be careful in endorsing [the change to 'a' purpose] because it holds out the potential that the government would seek FISA surveillance warrants—when it didn't have enough information to get a Title III order—but in which the foreign intelligence information to be obtained was remote or highly speculative"). *But see Homeland Defense: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 24–25 (2001) [hereinafter *Homeland*

though the administration stated that it would provide a legal analysis in support of the proposed change,[237] at a Senate Judiciary Committee hearing, Senator Dianne Feinstein urged Attorney General Ashcroft to consider an alternative formulation of the purpose requirement, to "substantial or significant purpose" rather than to "a purpose."[238] The Attorney General agreed to support a slight change in the proposal,[239] and the eventual Patriot Act amended FISA to provide that obtaining foreign intelligence must be "a significant purpose" of the surveillance.[240]

During the floor debate Senate Judiciary Committee Chairman Patrick Leahy acknowledged that "[p]rotection against these foreign-based threats by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA."[241] Senator Dianne Feinstein also opined that the objective of the change in the purpose language in the Patriot Act was to make it

> easier to collect foreign intelligence information . . . .
>
> . . . [I]n today's world things are not so simple. In many cases, surveillance will have two key goals—the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. . . .
>
> Rather than forcing law enforcement to decide which purpose is primary . . . this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.
>
> The effect of this provision will be to make it easier for law enforcement to . . . [use FISA] . . . where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution.[242]

These comments were embraced later by the Foreign Intelligence Surveillance Court of Review (FISCR) as supporting its interpretation of the change in the purpose language as to

Defense] (statement of John Ashcroft, Att'y Gen.).

237. *Intelligence to Prevent Terrorism Act*, *supra* note 233, at 21–22 (testimony of David S. Kris, Associate Deputy Att'y Gen.).

238. *Homeland Defense*, *supra* note 236, at 24–25 (statement of Sen. Dianne Feinstein, Member, Senate Committee on the Judiciary).

239. *Id.* at 25 (statement of John Ashcroft, Att'y Gen.).

240. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. at 291.

241. 147 Cong. Rec. S10,990, S11,004 (2001).

242. *Id.* at S10,586, S10,591.

practically eliminate any requirement that the government show a foreign intelligence purpose in its FISA applications.[243] However, the Leahy and Feinstein statements do not fairly reflect an intention, on their part or on the part of Congress as a whole, to change the overarching requirement of FISA that its processes be employed in pursuit of foreign intelligence. Senator Leahy simply acknowledged that it had been understood from the beginning of FISA that information collected under it could be used in prosecution, and Senator Feinstein noted that the statutory amendment will make it "easier" to use FISA in criminal cases, not that the foreign intelligence core of FISA was eliminated.[244]

The limited attention to this issue during floor debates and the lack of committee reports is unfortunate. In the determination to enact the new measures quickly after September 11, the details and complexities of FISA and careful consideration of the effects of its amendments were mostly lost on the reformers. From the beginnings of FISA in 1978, however, national security crimes provided a fusing point between foreign intelligence collection and law enforcement. The wall between the two types of surveillance thus had an open portal of sorts early on, and the Patriot Act change in the purpose language eased its use. In other words, the adjective "significant" has significant meaning in the amended FISA. There was movement of the standard, but not to such an extent that "a purpose" to collect foreign intelligence would suffice.

As part of a bundle of what some viewed as significant and controversial changes to existing legislation that the Bush administration effectively rushed through Congress, Congress enacted the purpose amendment and several others subject to a five-year sunset provision.[245] After enactment of the Patriot Act, the FISC responded to the first FISA applications filed under the revised Act by incorporating the augmented case-by-case 1995 OIPR procedures as formal minimization procedures that would apply to all future applications to the FISC.[246] Undaunted by the FISC order, the Justice Department immediately changed its guidelines to suspend the "chaperone" re-

243. *In re* Sealed Case, 310 F.3d 717, 732–33 (FISA Ct. Rev. 2002).

244. *See supra* notes 241–42 and accompanying text.

245. USA Patriot Act § 224, 115 Stat. at 295.

246. *In re Sealed Case*, 310 F.3d at 729; *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 619 (FISA Ct. Rev. 2002), *abrogated by In re Sealed Case*, 310 F.3d 717.

quirement that OIPR be present during any contacts between Criminal Division and FBI investigators concerning FISA matters.[247] Instead, OIPR and the FISC would thereafter receive briefings about such meetings.[248] More concrete changes came in March 2002, when new Intelligence Sharing Procedures were approved by Attorney General Ashcroft.[249] The new guidelines removed the information screening procedures and lifted the restriction that had been formally in place since 1995 on prosecutors or other law enforcement officials "directing or controlling" the use of FISA surveillance.[250] In addition, the new procedures encouraged complete sharing of information and advice and emphasized that "[t]he overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas."[251] Prosecutors are expected to have access to all information developed by the FBI in field intelligence investigations undertaken pursuant to FISA and prosecutors may advise the FBI about "all issues."[252] Although the Criminal Division, FBI, and OIPR are expected to meet and consult, OIPR is not required to be present when the other two meet.[253]

The new guidelines effectively dismantled the system that OIPR had in place since 1995. Although the 1995 procedures had erected information barriers that were not required by FISA, they assured that FISA was being used for its intended purpose and protected against tainting criminal cases with evidence obtained for the purpose of collecting foreign intelligence. The Ashcroft guidelines are, like their 1995 predecessor, for the most part not required by FISA, as amended by the Patriot Act.[254] The new information sharing provision in the Patriot Act did provide a statutory basis to remove barriers that had

247. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* 218 F. Supp. 2d at 619.

248. *In re Sealed Case*, 310 F.3d at 729.

249. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 615.

250. *In re Sealed Case*, 310 F.3d at 733–34.

251. Memorandum from John Ashcroft, Att'y Gen. of the United States, Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI to Dir. of the FBI, Assistant Att'y Gen. for the Criminal Div., Counsel for Intelligence Policy, and United States Attorneys (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html (hereinafter March 2002 procedures).

252. *Id.*

253. *Id.*

254. *See id.*

existed because of the previous procedures, including elimination of the OIPR as chaperone.[255] Although the legislative history surrounding the Patriot Act amendment to the purpose language does not clearly illuminate its purpose, the apparent aim was to facilitate information sharing between intelligence and law enforcement personnel after information is collected and, to a lesser extent, eliminate the incorrect but widespread belief that the use of FISA processes could undermine a subsequent or even contemporaneous prosecution.[256]

The change in the purpose language was really a change in emphasis only; it did not provide the basis for the elimination of the "direction or control" restriction on the Criminal Division. That single change in the procedures could be read to open up just the sort of misuse of FISA that was feared by the en banc FISC in its 2002 opinion.[257] Prosecutors that did not have grounds for a Title III warrant could urge intelligence investigators to expand their FISA surveillance parameters in pursuit of a criminal charge.[258] With such surveillance in place, FISA orders permit longer periods of surveillance, easier renewals, and less oversight than Title III.[259] The "direction or control" change was not required by the Patriot Act, and it apparently reflected the Attorney General's determination to move vigorously forward with the policy of prevention.

After the Attorney General approved the March 2002 procedures, the Department of Justice submitted a new application for FISA surveillance and, as part of the application, moved that the FISC vacate its minimization and wall procedures to the extent they are inconsistent with the new OIPR procedures.[260] In May 2002, the FISC issued a decision, joined by all seven judges of the court, that agreed with the request

255. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 504(a), 115 Stat. 272, 364–65 (codified at 50 U.S.C. §§ 1806(k), 1825(k)).

256. *See supra* Part III, notes 209–28 and accompanying text.

257. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624–25 (FISA Ct. Rev. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

258. *Id.* at 624.

259. *Compare* 50 U.S.C. § 1805(e) (2000) (allowing surveillance for a maximum time of ninety days, or one year if surveillance is targeted against a foreign power), *with* 18 U.S.C. § 2518(5) (2000) (allowing surveillance for a maximum time of thirty days).

260. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* 218 F. Supp. 2d at 613.

for the most part, but that rejected a portion of the new Justice Department guidelines and ordered new procedures to ensure the integrity of the underlying foreign intelligence purpose of FISA investigations.[261] The FISC opined that the new Justice Department procedures "appear to be designed to amend the law and substitute the FISA for [criminal law enforcement] electronic surveillances."[262] As the FISC interpreted FISA, the Justice Department procedures would gut the minimization requirements—designed to minimize the gathering of information about United States persons and to prevent its dissemination—if the Criminal Division could so easily use FISA-obtained electronic surveillance, and the Patriot Act did not affect those minimization requirements.[263] Instead of using minimization to determine the "need of the United States to obtain, produce, and disseminate foreign intelligence information,"[264] the new OIPR procedures would have the FISC balance the use of FISA materials "against the government's need to obtain and use evidence for criminal prosecution."[265]

According to the FISC, the limits it set on the OIPR procedures seek to avoid FISA activities where "criminal prosecutors direct both the intelligence and criminal investigations . . . [and] coordination becomes subordination of both investigations or interests to law enforcement objectives."[266] The court summed up the implications of the new procedures:

> [C]riminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute.[267]

The court feared that under the proposed procedures, prosecutors would have "every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information," including the looser probable cause standard and "use of the most highly advanced and highly intrusive techniques for intelligence gathering."[268] The

261. *Id.* at 626–27.

262. *Id.* at 623.

263. *Id.*

264. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A) (2000).

265. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court,* 218 F. Supp. 2d at 624.

266. *Id.* at 623–24 (emphasis omitted).

267. *Id.* at 624.

268. *Id.*

FISC concluded by striking two paragraphs of the OIPR procedures—those allowing criminal investigators to advise intelligence officials concerning "the initiation, operation, continuation, or expansion of FISA searches or surveillance"—and putting in their place a rule that law enforcement personnel should not "direct or control" the use of FISA procedures and a requirement that contacts between law enforcement and intelligence personnel working on parallel FISA investigations be monitored by OIPR.[269]

The three-judge FISA Court of Review abrogated this decision.[270] The FISCR harshly repudiated the FISC and wrote that its decision "not only misinterpreted and misapplied minimization procedures . . . [it] may well have exceeded the constitutional bounds that restrict an Article III court."[271] The FISCR rejected the idea that there had ever been in FISA any dichotomy between law enforcement and collection of foreign intelligence, before or after the Patriot Act.[272] According to the Court of Review, the simple change to "a significant purpose" by the Patriot Act removed any cause the FISC may have had to weigh the government's relative interests in law enforcement and foreign intelligence.[273] However, the Court also found that the Patriot Act, to a limited extent, codified such a dichotomy, and that it must be enforced.[274] Only if the government's "sole objective" is to obtain evidence of a past crime would the FISC properly deny an application.[275]

The FISCR reasoned that, because FISA defines the targets and information sought in close relation to national security criminal activity, any use of the information collected from FISA surveillance, including prosecution, is permitted.[276] However, the fact that "foreign intelligence information includes evidence of foreign intelligence crimes"[277] does not determine the limits on law enforcement use of FISA materials. Nor does the use of FISA surveillance for prosecution necessarily invali-

269. *Id.* at 623, 625 (emphasis omitted) (internal quotation marks omitted).

270. *In re* Sealed Case, 310 F.3d 717, 720, 746 (FISA Ct. Rev. 2002).

271. *Id.* at 731.

272. *Id.* at 725, 735.

273. *Id.* at 735.

274. *Id.* at 734–36.

275. *Id.* at 735–36 ("[T]he FISA process may not be used to investigate wholly unrelated ordinary crimes.").

276. *Id.* at 731.

277. *Id.* at 724.

date the FISA activities. If the gathering of foreign intelligence is a significant purpose of the surveillance, the later use of FISA-derived information in a criminal prosecution will not taint the evidence.[278] In short, the FISCR conflated what FISA information is used for with the purpose for using FISA.[279]

During the 1980's and early 1990's, some of the criminal convictions and appeals where FISA-derived evidence formed part of the basis for the prosecution upheld the use of the FISA evidence after finding that the surveillance was not "directed towards criminal investigation or the institution of a criminal prosecution."[280] Indeed, of the courts of appeal that reviewed FISA-related criminal convictions during this period, only the *Sarkissian* court "refuse[d] to draw too fine a distinction" between criminal and intelligence investigations."[281] The others endorsed the "primary purpose" test and, in doing so, presumed that a "wall" between the law enforcement and intelligence sides of an investigation existed.[282] However, none of these courts suppressed evidence and none contradict that in OIPR and the Justice Department during that period a robust coordination between intelligence and law enforcement officials was ongoing.[283] In short, the purpose requirement existed from the beginning, but the wall, misapprehended by the FISCR, came later.

After the sudden death of OIPR head Mary Lawton in 1993, Attorney General Janet Reno turned to her Florida colleague and Assistant U.S. Attorney in Miami, Richard Scruggs, to head OIPR.[284] Scruggs became concerned that there were no written guidelines governing contacts between the Criminal

278. *See supra* note 209 (citing decisions upholding the use of FISA procedures and FISA-derived evidence in criminal prosecutions).

279. *See* H.R. REP. NO. 95-1283, at 49 (1978) ("How this information may be used 'to protect' against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information . . . . Obviously, use of [foreign intelligence] as evidence in a criminal trial is one way the government can lawfully protect against . . . international terrorism.").

280. United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984) (quoting United States v. Megahey, 553 F. Supp. 1180, 1190 (E.D.N.Y. 1982)).

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

282. *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987); *Duggan*, 743 F.2d at 77.

283. *See* Supplemental Brief for the United States, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. Sept. 25, 2002) (No. 02-001), *available at* http://www.fas.org/irp/agency/doj/fisa/092502sup.html.

284. *See* DOJ Moves, 8 DOJ ALERT 11 (May 2, 1994).

Division and the intelligence side of FBI, and, upon discovering that a warrantless physical search on the home of Aldrich Ames had been conducted, he worried that the "primary purpose" analysis could be applied and thus compromise the criminal espionage case against Ames.[285] Soon, Scruggs began imposing information-sharing procedures for FISA materials on his own.[286]

Scruggs wrote a series of memoranda advocating guidelines for the separation of intelligence and criminal investigations, and in one of them he referred to his recommended procedures as establishing a "Chinese wall."[287] Thus, the origins of the 1995 guidelines and wall procedures that followed between then and 2002, reviewed above, were not, as the FISCR claimed, "shrouded in historical mist."[288] Nor did the wall's construction inside the Justice Department necessarily mean that FISA needed a statutory fix.

During his argument before the FISCR, Solicitor Ted Olson noted that when it comes to the meaning of the Patriot Act amendments to FISA, "we're not dealing with perfect clarity here."[289] Still, although the plain meaning of the amendment favors greater involvement by the Criminal Division in FISA investigations and more merged law enforcement and foreign intelligence investigations, the text does not support a construction that allows the Criminal Division to direct and control the FISA activities pertinent to an investigation.[290] The rule of construction disfavoring repeals by implication[291] applies here—why should a simple change from "the purpose" to "a significant purpose" be construed to overturn twenty-five years of FISA understandings that the objective of the procedures is to permit secret gathering of foreign intelligence? The change from "the" to "a" shows explicit recognition of the overlap between law enforcement and foreign intelligence, and "significant" qualifies the quantum of foreign intelligence that

285. *See* 9/11 COMMISSION REPORT, *supra* note 167, at 78; 2004 OIG REPORT, *supra* note 168, at 25.

286. 9/11 COMMISSION REPORT, *supra* note 167, at 78.

287. 2004 OIG REPORT, *supra* note 168, at 25–26.

288. *In re* Sealed Case, 310 F.3d 717, 720, 746 (FISA Ct. Rev. 2002).

289. Transcript of Oral Argument at 55, *In re* Sealed Case, 310 F.3d 717 (No. 02-001), *available at* http://www.fas.org/irp/agency/doj/fisa/hrng090902.htm.

290. *See* Banks, *supra* note 16, at 1179–81.

291. *See* Peter Raven-Hansen & William C. Banks, *Pulling the Purse Strings of the Commander in Chief*, 80 VA. L. REV. 833, 855–56 (1994).

must be sought.[292] The FISCR decision considerably weakened the foreign intelligence core of FISA.

When the FISCR convened in 2002, it was undeniable that national security investigations often have multiple purposes. Moreover, because Congress has made many terrorist activities crimes, there is more than ever an overlap between foreign intelligence and law enforcement, even within the same investigation and targets.[293] Criminal prosecution supported by effective intelligence investigations can be an effective counterterrorism tactic.[294] Still, as interpreted by the Court of Review, FISA can permit the government to skirt the statutory and constitutional protections afforded those subject to law enforcement investigations.[295] FISA was created as a system for surveillance for foreign intelligence, not for solving crimes.[296] Outside that exceptional arena of foreign intelligence, the Constitution before and after 1978 requires Fourth Amendment notice to targets, Sixth Amendment confrontation of evidence, and First Amendment freedom of expression without a chill from the specter of looming FBI surveillance.[297]

So understood, the wall is an essential part of the larger context for managing and implementing FISA, whether or not the pre- or post-Patriot Act language literally requires such separation.[298] If something like the wall procedures are not in place, FISC-approved surveillance may violate the Constitution when the FBI begins an investigation principally to build a criminal case.[299]

---

292. *See* Banks, *supra* note 16, at 1177–81.

293. *See* Banks & Bowman, *supra* note 1, at 9.

294. *See id.*

295. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624 (FISA Ct. 2002), *abrogated by In re* Sealed Case, F.3d 717 (FISA Ct. Rev. 2002).

296. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1320 (2004).

297. *See id.* at 1339–41 (discussing how the full protections of the American criminal justice system apply to targets of wiretaps in ordinary law enforcement actions).

298. *See* RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 112–13 (2006) ("[The FBI] incorrectly believes that intelligence is a natural outgrowth of traditional criminal investigative practices."); *id.* at 134 ("The Bureau has a history of redefining criminal investigations as intelligence operations in order to use FISA warrants and NSA intercepts to obtain information for use in drug or other ordinary-crimes investigations.").

299. *See* Swire, *supra* note 296, at 1361.

B. AVOIDANCE OF FISA: THE TERRORIST SURVEILLANCE PROGRAM

On December 11, 2005, the New York Times publicly revealed what the Bush administration later called the Terrorist Surveillance Program (TSP), when it reported that President Bush secretly authorized the National Security Agency (NSA) to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without judicial approval.[300] In a letter from the Justice Department to the congressional intelligence committees a few days later, the Assistant Attorney General stated that a secret order from the President authorized the program shortly after September 11, and that the surveillance is aimed at "certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization."[301] Since beginning the program, NSA has monitored the telephone and e-mail communications of thousands of persons inside the United States where one end of the communication is outside the United States, without warrants.[302] Aside from defending the program as "crucial to our national security,"[303] the President lamented "the unauthorized disclosure of this effort . . . . Revealing classified information is illegal, alerts our enemies, and endangers our country."[304]

While the Justice Department launched an investigation of the leak,[305] the administration defended the legality of the TSP in the face of widespread criticism in Congress, lawsuits by civil liberties organizations and defendants who have challenged their previous pleas or convictions, and countless op-ed attacks, blog debates, and other commentary.[306] Many of us wondered—in light of the win/loss record of the government before the

300. *See* Risen & Lichtblau, *supra* note 23. Although details of the NSA program remain classified, press reports indicate that data mining and traffic analysis technologies are being employed. Shane Harris, *How Does the NSA Spy?*, NAT'L L.J., Jan. 20, 2006, at 47, 49.

301. Letter from William E. Moschella to Pat Roberts, *supra* note 24, at 1.

302. Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253, 289 (2006).

303. Letter from William E. Moschella to Pat Roberts, *supra* note 24, at 1.

304. *Id.*

305. Toni Locy, *Justice Dept. Opens Domestic Spying Probe*, BREITBART.COM, Dec. 30, 2005, http://www.breitbart.com/news/2005/12/30/D8EQLIAGB.html.

306. *See infra* notes 300–05 and accompanying text.

FISC, why would the administration not rely on a sure thing? How could the President have stated in 2004 that "any time you hear the United States government talking about wiretap, it requires . . . a court order. Nothing has changed. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so."[307]

When critics pointed out the obvious—that secret electronic surveillance for foreign intelligence inside the United States is provided for by FISA—the administration defended the decision not to rely on the FISA processes. Given the expansiveness of the definition of "electronic surveillance" in FISA,[308] the "exclusivity" provisions of FISA and the companion criminal enforcement statute,[309] and the criminal penalties for unauthorized electronic surveillance,[310] the administration faced an uphill legal climb. FISA provides criminal penalties for anyone who engages in electronic surveillance "not authorized by statute."[311] The administration has argued that the Authorization for the Use of Military Force (AUMF) constitutes the necessary authorization within the meaning of the FISA "authorized by statute" provision.[312] The text and legislative history clearly reveal, however, that the purpose of the FISA provision is to provide security to intelligence personnel who act in accordance with FISA, not to immunize them if they violate the law.[313] The "statute" referred to in section 1809 is FISA, or Title III.[314] Similarly, the administration's claims of AUMF authority would make the exclusivity provision in FISA meaningless.[315]

Attorney General Gonzales emphasized the need for "speed and agility" in making judgments about particular intercepts,

307. President's Remarks in a Discussion on the PATRIOT Act in Buffalo, New York, 40 WEEKLY COMP. PRES. DOC. 641 (Apr. 20, 2004).

308. 50 U.S.C. § 1801(f) (2000 & Supp. 2004).

309. 18 U.S.C. § 2511(2)(e)–(f) (2000 & Supp. II 2003).

310. 50 U.S.C. § 1809(a)(1) (2000 & Supp. III 2004).

311. *Id.*

312. Letter from William E. Moschella to Pat Roberts, *supra* note 24, at 2.

313. *See generally NSA III: War Time Executive Power and the FISA Court: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 812 (2006) [hereinafter Statement of David S. Kris] (statement of David S. Kris, Senior Vice President, Time Warner Inc.), *available at* http://www.balkin.blogspot.com/kris.testimony.pdf (discussing how Congress intended for FISA's procedures to be the exclusive means for conducting foreign electronic surveillance).

314. *Id.*

315. *Id.*

and he maintained that "navigat[ing] through the FISA process" would delay the work and produce "critical holes in our early warning system."[316] Acknowledging the emergency authorizations expressly contemplated in FISA, the Attorney General implied that the required procedures were too burdensome or that, perhaps, they could not be met. Gonzales noted that he would have to sign off on each application, as would the lawyers at NSA and Justice Department, after determining that "all provisions of FISA have been satisfied."[317] Although Gonzales did not clearly state whether it was the anticipated failure to meet the probable cause requirement of FISA or the burden of work to meet the seventy-two-hour deadline that led the administration to go outside FISA, Deputy Director of National Intelligence, General Michael V. Hayden stated at about the same time that the administration had unilaterally adopted a "reasonable suspicion" standard in applying the TSP because the "probable cause" standard in FISA is, in the words of one commentator, "too onerous."[318]

The administration passed up an invitation to revise the predicate probable cause standard in 2002. Legislation proposed by Senator Michael DeWine would have substituted a "reasonable suspicion" standard for "probable cause" to believe that the surveillance target is a foreign power or agent of a foreign power for FISA surveillance requests involving non-United States persons.[319] When asked to advise Congress on the proposed amendment, James A. Baker, then head of OIPR in the Justice Department, gatekeeper of the FISA process, opined that the Patriot Act extension of the emergency surveillance window from twenty-four to seventy-two hours "has allowed us to make full and effective use of FISA's pre-existing emergency provisions to ensure that the government acts swiftly to re-

316. Alberto R. Gonzales, Att'y Gen., Prepared Remarks for Attorney General Alberto R. Gonzales at the Georgetown University Law Center (Jan. 24, 2006) *available at* http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html [hereinafter Gonzales, Georgetown Remarks].

317. *Id.*

318. Unclaimed Territory, The Administration's New FISA Defense is Factually False, http://glenngreenwald.blogspot.com/2006/02/adminstrations-new-fisa-defense-is.html (Jan. 24, 2006, 16:11 EST) [hereinafter Unclaimed Territory].

319. *Amendments to the Foreign Intelligence Surveillance Act: Hearing on S. 2586 and S. 2659 Before the Select Comm. on Intelligence*, 107th Cong. 12 (2002) (statement of Sen. Michael DeWine), *available at* http://intelligence.senate.gov/fisa.pdf.

spond to terrorist threats."[320] Baker testified that the Justice Department would not support Senator DeWine's proposal—because the probable cause standard was likely not an obstacle to effective use of FISA, and because the Department worried that the reasonable suspicion standard might be unconstitutional.[321] The executive branch thus expressed concern that a lowered standard might be unconstitutional at the same time they were engaged in just that practice. Admittedly, the DeWine proposal would have loosened the predicate only for non-United States persons. The TSP does not distinguish United States persons from others, and it forgoes the FISC oversight that the lower standard would continue to provide.

Attorney General Gonzales also asserted that seeking legislative authority for the TSP would have tipped off the enemies and let them know what surveillance activities we were pursuing.[322] Although Gonzales stated that the administration had been "advised that [it] would be difficult, if not impossible"[323] to obtain such an amendment to FISA, he apparently referred not to the political or legal difficulties such a proposal would face, but to the concern that such an amendment could not be obtained "without jeopardizing the existence of the program."[324] For example, once the administration admitted the program's existence and cautioned that the program only intercepted international calls, in theory those who subject to the surveillance could evade the program through countermeasures, such as use of VoIP (Voice over Internet Protocol) phones with U.S. numbers but used abroad.[325]

Putting to one side the possibility of legislation being considered in executive session, with classified information secured and sources and methods protected pursuant to House and Senate rules, and despite some briefings on the TSP to se-

320. *Id.* at 23 (statement of James A. Baker, Counsel for Intelligence Policy, Dep't of Justice).

321. *Id.*

322. Press Briefing, Alberto R. Gonzales, Att'y Gen., Gen. Michael V. Hayden, Principal Deputy Dir. of Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html [hereinafter Press Briefing, Gonzales & Hayden].

323. *Id.*

324. *Id.*

325. VoIP telephone technology permits the user to mask his location because the phone number where the call originates may be a U.S. number from wherever the call is placed. *See* FCC, Voice over Internet Protocol Frequently Asked Questions, http://www.fcc.gov/voip/ (last visited Apr. 13, 2007).

lected members, Congress did not know what NSA was doing in the TSP. By statute the President is required to keep the congressional intelligence committees "fully and currently informed" of the intelligence activities of the United States, including any "significant anticipated intelligence activity."[326] For covert actions, the President is permitted, in order "to meet extraordinary circumstances affecting vital interests of the United States" to limit reporting to select members of the Congressional intelligence committees and the leaders of the House and the Senate—"Gang of Eight."[327] Reportedly, the TSP was briefed only to the Gang of Eight, and the eight were forbidden from sharing information about the program with colleagues, including members of the intelligence committees.[328] However, as described by the administration, the TSP is an intelligence collection program, not a covert action program. As defined by statute, covert action does not include those "activities the primary purpose of which is to acquire intelligence."[329] As such, the TSP had to be disclosed to the intelligence committees.

The only plausible legal cover for the truncated notice and briefing to Congress is that the reporting requirements for intelligence collection activities are binding "[t]o the extent consistent with due regard for the protection of unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters."[330] If that is the explanation, however, some form of limited notice would be justified only for the particularly sensitive aspects of the program, not the fact of its existence.

The administration claims that the TSP was regularly vetted by lawyers at the Department of Justice.[331] Newsweek magazine reported, however, that dissension over the TSP inside the Department spilled over when then Deputy Attorney General James Comey refused to authorize the NSA program during a period when Attorney General Ashcroft was in the hospital with a serious medical condition.[332] When Comey re-

326. 50 U.S.C. § 413(a)(1) (2000 & Supp. III 2004).

327. *Id.* § 413b(c)(2).

328. Press Release, Sen. John D. (Jay) Rockefeller, IV, Vice Chairman Rockefeller Reacts to Reports of NSA Intercept Program in United States (Dec. 19, 2005), *available at* http://www.senate.gov/~rockefeller/news/2005/pr121905a.html.

329. 50 U.S.C. § 413b(e).

330. *Id.* § 413a(a).

331. *See* Press Briefing, Gonzales & Hayden, *supra* note 322.

332. Daniel Klaidman et al., *Palace Revolt: They Were Loyal Conservatives,*

fused to sign off on the program, a White House delegation, including then White House Counsel Gonzales, visited Ashcroft in the hospital to appeal Comey's decision, with apparent success.[333] Vetted or not, administration admissions that wholly domestic calls might have been monitored in the larger sweep for terrorist activities contradict the claim that the only calls to or from persons and locations overseas are monitored.[334]

Those who characterize the TSP as a complex and technologically advanced data mining program that simply cannot be fitted inside the obsolete structure of FISA take a different path.[335] Apart from the Attorney General and the President falling back on the need for "speed and agility," and stating that the war we are fighting is "a different war," many advocates of the TSP say, quite simply, that the law has failed to keep up with the technology.[336] However, according to General Hayden, who was head of NSA when the program was implemented, TSP "is not a driftnet over Dearborn or Lackawanna or Freemont, grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools. . . . This is targeted and focused."[337] Hayden claimed the surveillance was limited to "international calls and only those we have a reasonable basis to believe involve al Qaeda or one of its affiliates."[338] Hayden was blunt: "we're not there sucking up coms and then using some of these magically alleged keyword searches—Did he say 'jihad'?"[339] Instead, a shift supervisor at NSA substitutes for a federal judge.[340] She decides what part of the product of the data-mining merits further targeted surveillance, and the

and Bush Appointees. They Fought a Quiet battle to Rein in the President's Power in the War on Terror. And They Paid a Price for It. A Newsweek Investigation, NEWSWEEK, Feb. 6, 2006, at 34, 39.

333. *Id.*

334. *See* Stewart M. Powell, *White House Acknowledges Some Taps Wholly Domestic*, S.F. CHRON., Dec. 22, 2005, at A6.

335. Press Briefing, Gonzales & Hayden, *supra* note 322.

336. *See, e.g.*, Richard A. Posner, Op-Ed., *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16; K.A. Taipale & James Jay Carafano, Op-Ed., *Fixing Surveillance*, WASH. TIMES, Jan. 24, 2006, *available at* http://www.washingtontimes.com/commentary/20060124-104527.

337. General M. Powell, Principal Deputy Dir. of Nat'l Intelligence, Address to the National Press Club (Jan. 23, 2006), *available at* http://www.fas.org/irp/news/2006/01/hayden012306.html.

338. *Id.*

339. *Id.*

340. *Id.*

standard she employs in making those decisions is reasonable suspicion instead of probable cause.[341]

The legality of the TSP was thus defended by the Administration at the same time that it admitted, in effect, that the program does not comply with FISA. Nor did the Administration fulfill congressional reporting requirements for intelligence collection activities. Whether officials substituted a "reasonable suspicion" standard or some other criterion in deciding who to target with TSP, the substitution of an NSA employee for a federal judge as the gatekeeper is a startling departure from the regularized procedures of FISA.

C. SYNTHESIZING THE POST-SEPTEMBER 11 DEVELOPMENTS: THE DEATH OF FISA

The inter-branch compromise that produced FISA contains a series of interlocking elements. FISA required a form of prior judicial approval to intercept electronic communications inside the United States, except in emergencies.[342] The interception had to be targeted at particular persons or places related to suspected terrorism or espionage.[343] The predicate for issuing a court order was a showing of probable cause of foreign agency and that foreign intelligence will be acquired,[344] and Congress determined in 1978 that these parameters were the exclusive means for carrying our electronic surveillance for foreign intelligence inside the United States.[345] A fully informed Congress was to oversee all of the above.[346]

Part B showed that amendments to the Act, judicial decisions, or executive practice have already undercut some of these elements of FISA. Others remained arguably intact until the TSP emerged, and Congress prepared to bargain away the important remaining pieces of FISA. The two sea-change developments explored here—dismantling of the foreign intelligence "purpose" screening requirements and the NSA Terrorist Surveillance Program—should not be understood as the only causes of the death of FISA. Larger institutional and societal

341. *Id.*
342. 50 U.S.C. § 1805(f) (2000).
343. *Id.* § 1805(a)(3).
344. *Id.*
345. 18 U.S.C. § 2511(2)(f) (2000 & Supp. III 2004).
346. 50 U.S.C. §§ 413(a)(1), 1807–1808 (2000).

atmospherics, particularly in the last five years, place the demise of FISA in context.

An overriding aura of emergency has driven the post-September 11 counter-terrorism programs, including the Patriot Act,[347] the FISCR decision,[348] and the NSA program.[349] The Bush administration effectively has sustained the emergency through its global war on terrorism and the war in Iraq, and Congress and the courts have altered their perspectives in light of it.[350] One result is that the central lesson of the *Keith* case has been lost—that the societal interests in security and civil liberties must be balanced, with the participation of the federal courts.[351] In a 2006 insider's account by Professor John Yoo of his experiences inside the Justice Department in helping to shape the post-September 11 programs, Yoo maintained that "FISA . . . was created specifically to hamstring the executive branch in favor of civil liberties."[352] Professor Yoo's revisionist history is emblematic of the change in orientation of government after September 11, a change also expressed in the opinion of the FISA Court of Review. In rejecting the opinion signed by all of the FISC judges, the Court of Review essentially took the core out of FISA when it opined that the Justice Department would have free rein in deciding when to use the FISA procedures.[353]

During the same period, Congress effectively ceded its role in leadership.[354] The executive branch devised the policies it wished to follow after September 11, and it set in place the programs and enforcement activities to meet the policy objectives.

347. Pub. L. No. 107-56, 115 Stat. 272 (2000).

348. *In re* Sealed Case, 310 F.3d 717, 720, 746 (FISA Ct. Rev. 2002).

349. *See* Harris, *supra* note 300, at 47.

350. *See* Risen & Lichtblau, *supra* note 23, at A16 (discussing how the NSA program reflects a major shift in American intelligence gather practices).

351. *See id.* at A1 (discussing the difficulty of identifying a line between national security interests and the rights of Americans against undue searches).

352. YOO, *supra* note 206, at 73.

353. *See In re* Sealed Case, 310 F.3d at 731–32.

354. *See* Norman J. Ornstein & Thomas E. Mann, *When Congress Checks Out*, FOREIGN AFF., Nov.–Dec. 2006, at 67, 68 ("In the past six years, Congressional oversight of the executive . . . on foreign and national security policy . . . has virtually collapsed.").

1. The Wall

In early oversight hearings on the implementation of FISA, Senator Malcolm Wallop expressed the view that the "net effect [of FISA] has been to confuse intelligence gathering with criminal law" and that it is "nonsense" to attempt a formula for comprehensive surveillance of those who constitute a security threat.[355] Nonetheless, the FISA process worked reasonably well. Evidence impermissibly gathered through FISA surveillance did not taint affected criminal prosecutions because the "primary purpose" rule was workable in practice. At the same time, direction and control from the law enforcement side of the Justice Department did not encumber the foreign intelligence investigators.

Within days of September 11, FISA became a convenient foil for those seeking to explain our government's failure to stop the hijackers. It became part of the urban myth surrounding September 11 that the FISA wall caused the government to lose contact with suspected terrorists,[356] and most notoriously, that the FISA wall was blamed for the failure to secure FISA surveillance of then supposed twentieth hijacker Zacarias Moussaoui's laptop computer in the days and weeks before September 11.[357] Moussaoui was arrested on an immigration overstay charge in August 2001. A flight instructor at a flight training school in Minnesota grew suspicious when Moussaoui said that he wanted to learn to fly large jet aircraft, but that he had no interest in becoming a commercial pilot.[358]

355. SENATE SELECT COMM. ON INTELLIGENCE, IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, S. REP. NO. 97-691, at 9–10 (1982).

356. *See* YOO, *supra* note 206, at 72 ("I was asked to work on fixing the most important defect in our intelligence laws—the legal 'Wall' . . . . the Wall had played a role in our failure to stop the 9/11 attacks.").

357. *See* JOINT INQUIRY STAFF, 107TH CONG., THE FBI'S HANDLING OF THE PHOENIX ELECTRONIC COMMUNICATION AND INVESTIGATION OF ZACARIAS MOUSSAOUI PRIOR TO SEPTEMBER 11, 2001, at 14 (2d Sess. 2002) (statement of Eleanor Hill, Staff Dir., Joint Inquiry Staff) [hereinafter JOINT INQUIRY STAFF MEMORANDUM], *available at* http://www.fas.org/irp/congress/2002_hr/092402hill_pdf.

358. Press Release, Pan Am Int'l Flight Acad., Pan Am International Flight Academy Statement to the News Media, http://www.panamacademy.com/template_press.asp?id=119 (last visited Apr. 13, 2007). The Minneapolis Star Tribune quoted the flight instructor as telling the FBI, "Do you realize how serious this is? . . . This man wants training on a 747. A 747 fully loaded with fuel could be used as a weapon!" Greg Gordon, *A Persistent Suspicion: Eagan Flight Trainer Wouldn't Let Unease About Suspect Rest*, STAR TRIB., Dec. 21, 2001, at A1 (internal quotation marks omitted).

When field agents sought the headquarters' approval for a FISA surveillance order, they were turned down, because there was insufficient information connecting Moussaoui to a foreign power.[359] However, the headquarters' agents only orally briefed the lawyers responsible for making the foreign agency recommendation. If the agents had searched FBI computer records relevant to the Moussaoui request, they would have had access to a July 2001 memorandum from a Phoenix agent that warned about the potential dangers of al Qaeda affiliates seeking training at U.S. flight schools.[360] FBI personnel did not follow up on the memorandum, and no senior officials at the Bureau saw the memorandum before September 11.[361] In addition, the headquarters' staff lawyers apparently mistakenly advised the Minneapolis agents that foreign agency required a link to a terrorist organization on the State Department list of terrorist organizations.[362] At about the same time, the FBI received a classified cable from a French intelligence agency that warned the Moussaoui had "Islamic extremist beliefs."[363] If the French intelligence had been coupled with the Phoenix memorandum, the fact-sensitive foreign agency inquiry might have produced a different outcome. But the two sources together would have only suggested that Moussaoui was affiliated with al Qaeda and thus had a connection to a foreign power.[364]

The Minnesota agents did not open a criminal investigation that would have permitted a search of Moussaoui's laptop because FBI headquarters believed that the agents lacked sufficient probable cause of a crime.[365] A criminal case was opened and a FISA order was obtained, but only after the September

359. JOINT INQUIRY STAFF MEMORANDUM, *supra* note 357, at 17.

360. *See* Shelby, *supra* note 15, at 29.

361. *Id.* at 29–30.

362. *Id.* at 53.

363. David Johnston & Philip Shenon, *F.B.I. Curbed Scrutiny of Man Now a Suspect in the Attacks*, N.Y. TIMES, Oct. 6, 2001, at A1. Professor Yoo slightly alters the reported facts regarding Moussaoui and writes that Moussaoui "had connections to extreme Islamic groups." YOO, *supra* note 206, at 80. It was precisely the lack of demonstrated ties to any foreign power that caused headquarters to decline to pursue a FISA application. 9/11 COMMISSION REPORT, *supra* note 167, at 274.

364. 9/11 COMMISSION REPORT, *supra* note 167, at 272. On September 13, the British government received and passed on to the United States intelligence that Moussaoui had attended an al Qaeda training camp in Afghanistan. *Id.* Obviously, if this information had been available in August, the predicate for FISA surveillance would have existed. *Id.* at 275.

365. *Id.* at 273–74.

11 attacks.[366] Although the 9/11 Commission later found that a "maximum U.S. effort" to investigate Moussaoui "might have brought investigators to the core of the 9/11 plot," the Commission refused to blame any shortcomings in investigating Moussaoui on the "purpose" requirement or the wall procedures implementing FISA.[367] Nonetheless, the Moussaoui story emerged as a symbol of the supposed dysfunctional state of intelligence sharing in Washington and it became part of the urban myth that helped spur enactment of the Patriot Act.[368]

Professor John Yoo helped reinforce the mythical stature of the wall. He blamed "[s]trict enforcement of the Wall between law enforcement and foreign intelligence" for preventing the CIA from sharing photos with the FBI showing a meeting between eventual hijacker Khalid al Mihdhar and al Qaeda operatives involved in the bombing of the USS Cole.[369] According to Professor Yoo, because the *Cole* bombing investigation was run by the FBI Criminal Division, the CIA refused to share its intelligence photos "because of the Wall."[370] When Mihdhar entered the U.S. again on July 4, 2001, CIA and FBI counterterror agents knew of his al Qaeda connection and tried to locate him, but they refused to share their information with the FBI criminal agents in New York.[371] The FBI criminal agent working on the *Cole* investigation replied angrily in an e-mail message that "whatever has happened to this—someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'"[372]

The FBI agent's frustration is palpable and understandable, but Professor Yoo's attribution of blame to FISA or any legal procedures implementing FISA is misplaced. After hearing testimony from the relevant officials, including Attorney General Ashcroft,[373] the 9/11 Commission concluded that in the

366. *Id.* at 276.

367. *Id.* (stating that the connection between Moussaoui and al Qaeda was "not an easy trail to find").

368. *See generally* Craig S. Lerner, *Calling a Truce in the Culture Wars: From Enron to the CIA*, 17 STAN. L. & POL'Y REV. 277, 277–78 (2006) (discussing the public's view of the intelligence failure).

369. YOO, *supra* note 206, at 80.

370. *Id.*

371. *Id.* at 80–81.

372. 9/11 COMMISSION REPORT, *supra* note 167, at 271.

373. *Id.* at 439 (listing the witnesses who testified in front of the Commission).

Mihdhar case "everyone involved was confused about the rules governing the sharing and use of information gathered in intelligence channels."[374] A criminal investigation had already been opened on the *Cole* bombing, and Mihdhar could have been investigated and tracked as part of that case.[375] Unfortunately, either the FBI intelligence agent that possessed information about Mihdhar or a Bureau lawyer who advised her incorrectly determined that the intelligence could not be shared with the criminal investigators.

The FISA wall procedures were designed to protect against using the secretive foreign intelligence collection process in order to build a criminal case.[376] FISA never stood in the way of the sharing of criminal information with intelligence investigators.[377] Nor did it apply to the sharing of intelligence information with criminal investigators, so long as the sharing met the foreign intelligence purpose rule.[378]

The 1995 procedures governed sharing with prosecutors, not other FBI agents.[379] Ironically, the intelligence concerning Mihdhar came from NSA and was ordered by Attorney General Reno, pursuant to Executive Order 12,333.[380] In what the 9/11 Commission called an "overabundance of caution. . . [d]uring the millennium crisis,"[381] the Attorney General ordered overseas electronic surveillance of three U.S. persons with the proviso that the results not be shared with criminal investigators or prosecutors without the permission of OIPR.[382] Even though the restrictions did not apply to the Mihdhar surveillance, NSA placed the restrictions on all of the agency's bin Laden-related reporting.[383] Attorney General Ashcroft testified before the 9/11 Commission that these information sharing problems were attributable to the 1995 guidelines.[384] The Commission disagreed and found that, "[w]hatever the merits of the . . . 1995 . . . procedures . . . , they did not apply to the information the analyst

374. *Id.* at 271.
375. *Id.*
376. Banks, *supra* note 16, at 1152–53.
377. 9/11 COMMISSION REPORT, *supra* note 167, at 538 n.80.
378. *Id.*
379. 2004 OIG REPORT, *supra* note 168, at 27.
380. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981).
381. 9/11 COMMISSION REPORT, *supra* note 167, at 537, n.71.
382. *Id.*
383. *Id.*
384. *Id.* at 539 n.83.

decided she could not share with the criminal agent."[385] In short, "a bureaucratic culture," not legal restrictions, prevented the sharing of intelligence that might have led investigators to at least one of the September 11 hijackers before the attacks.[386]

Once the Patriot Act was implemented, the supposed gains in counter-terrorism prosecutions that came from lowering the wall were showcased in the February 2003 indictment of Sami Al-Arian and others in Florida, based on allegations that they financed suicide bombings in Israel.[387] Attorney General Ashcroft maintained at the news conference that the investigators had been "stymied" by restrictions on the use of foreign intelligence in criminal cases and that the expanded powers granted by the Patriot Act allowed them to proceed with the prosecution.[388] In fact, the FBI began investigating Al-Arian in the early 1990s and began FISA-approved electronic surveillance in the same period.[389] Some of the material that prosecutors used to bring their indictment was ten years old, and it included much that is foreign intelligence as defined in FISA.[390] It was false to imply that the pre-Patriot Act FISA inhibited building a criminal case against Al-Arian and his co-conspirators.[391] So long as the investigators sought the FISA surveillance for the purpose of collecting foreign intelligence, the Department did not run afoul of FISA and it was not hamstrung by FISA in bringing its criminal prosecution.[392]

As the Patriot Act sunsets loomed in 2005 and then were extended by temporary legislation into early 2006,[393] serious consideration was never given to revisiting the "significant

385. *Id.*

386. *Id.* ("Simply put, there was no legal reason why the information the analyst possessed could not have been shared with the criminal agent.").

387. Eric Lichtblau & Judith Miller, *Indictment Ties U.S. Professor to Terror Group*, N.Y. TIMES, Feb. 21, 2003, at A1.

388. *See* Banks *supra* note 16, at 1188; John Ashcroft, U.S. Att'y Gen., Press Conference (Feb. 20, 2003) (transcript available at http://transcripts.cnn.com/TRANSCRIPTS/0302/20/se.04.html).

389. Banks, *supra* note 16, at 1188.

390. *Id.*; *see also* 50 U.S.C. 1801(e) (2000) (defining foreign intelligence).

391. Banks, *supra* note 16, at 1188–89.

392. *Id.* at 1189.

393. Emergency legislation first extended the sunset provisions until February 3, 2006. Extension of the Sunset of Certain Provisions of the USA PATRIOT Act, Pub. L. No. 109-160 § 1, 119 Stat. 2957 (2005). A second act extended the provisions until March 10, 2006. Extension of Sunset of Certain Provisions of the USA PATRIOT Act, Pub. L. No. 109-170 § 1, 120 Stat. 3 (2006).

purpose" language or to clarifying the reason for the "purpose" language. Instead, after compromises were made to revise the authorities for National Security Letters and business records,[394] the sunset on the significant purpose provision and twelve of fourteen other Patriot Act authorities subject to sunset were simply repealed.[395]

The reauthorization and lifting of the sunset on "significant purpose" only underscores that the Patriot Act change was not legally necessary or sufficient to eliminate the wall. The amendment was not necessary because the obstacles to sharing information or integrating data are not the product of legal rules.[396] A change would not have been sufficient to overcome the Fourth Amendment requirement that relaxed approval processes for electronic surveillance be reserved for when the purpose is collection of foreign intelligence.[397]

The Supreme Court has never upheld warrantless electronic surveillance inside the United States.[398] If criminal prosecutors were permitted to initiate, direct, and control warrantless electronic surveillance and then use the information so collected as prosecution evidence, they would be circumventing the traditional Fourth Amendment requirements by using alternate procedures allowed specifically for foreign intelligence to develop a criminal prosecution.[399] However, the Supreme

394. CHARLES DOYLE, CONG. RESEARCH SERV., USA PATRIOT ACT: BACKGROUND AND COMPARISON OF HOUSE- AND SENATE-APPROVED REAUTHORIZATION AND RELATED LEGISLATIVE ACTION 12–13 (2005) (listing the differences between the House and Senate resolutions).

395. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 § 102(a), 120 Stat. 192, 195 (2006). A new sunset of December 31, 2009 was approved for surveillance of suspected "lone wolf" terrorists. *Id.* § 103.

396. 9/11 COMMISSION REPORT, *supra* note 167, at 539 n.83 (stating that there was "no legal reason" why information could not be shared).

397. *Compare* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 321 (1972) (rejecting warrantless wiretapping of a domestic group engaged in national security crimes), *and* Katz v. United States, 389 U.S. 347, 358–59 (1967) (no exception to the traditional warrant requirement for electronic surveillance), *and* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH L. REV. 1264, 1299–1304 (2004) (arguing for a return to the pre-Patriot Act "primary purpose" standard for FISA surveillance), *with* AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE 31 (1997) (claiming that the Fourth Amendment requires reasonableness, not probable cause and a warrant).

398. *See, e.g.*, *Keith*, 407 U.S. at 321.

399. *Id.* at 316–17 ("[Unreviewed discretion] may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.").

Court's recognized in the *Keith* decision that traditional Fourth Amendment warrant and probable cause requirements may not be compatible with the needs of national security surveillance and that different standards might be constitutionally permissible if they are reasonable.[400] FISA incorporated these concerns and reflects Congress's recognition of the real world difficulties of separating the foreign intelligence and law enforcement components of an investigation concerning international terrorism. Although the prosecution does not actually initiate and direct a FISA investigation, the significant purpose amendment to FISA does allow prosecutors access to FISA-derived evidence in the criminal case.[401]

Nor did FISA, before or after the Patriot Act, prevent the government from using FISA-authorized surveillance against a defendant in a criminal case.[402] In fact, evidence obtained through FISA surveillance has often been used in criminal prosecutions.[403] In a number of cases discussed in this Article, convicted terrorists have appealed in part on grounds that incriminating evidence obtained through FISC-approved surveillance should not have been admitted because it was acquired in order to build the criminal cases, and the criminal warrant process was not followed.[404] The courts of appeals have consistently rejected these arguments.[405] The *Sarkissian* court refused "to draw too fine a distinction between criminal and intelligence investigations," and it noted that the investigation of international terrorism necessarily requires investigation of criminal activities.[406] So long as the purpose of launching the FISA surveillance is to obtain foreign intelligence, the fact that the government later chooses to prosecute the target does not undercut the lawfulness of the FISA surveillance.

400. *See id.* at 322–23.

401. *See* Swire, *supra* note 296, at 1330–31 (noting that the amendment was promulgated to allow information sharing between criminal and foreign intelligence investigations).

402. Banks, *supra* note 16, at 1189.

403. *See, e.g.*, United States v. Hammoud, 381 F.3d 316 (4th Cir. 2004) (en banc), *vacated*, 543 U.S. 1097 (2005); United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

404. *See, e.g.*, *Hammoud*, 381 F.3d at 332; *Sarkissian*, 841 F.2d at 961; *Duggan*, 743 F.2d at 64–65.

405. *Hammoud*, 381 F.3d at 333–34; *Sarkissian*, 841 F.2d at 964–65; *Duggan*, 743 F.2d at 78.

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

To argue, as some did in the Patriot Act reauthorization debates, that the modern blending of crimes and foreign intelligence threats should be reason enough to eliminate the wall provisions.[407] However, this fails to take into account that the purpose requirement focuses on the investigators' reason for seeking a FISA order, not on what is done with the product of the surveillance.[408] If the purpose of the investigation is to prosecute, FISA should be unavailable, given its requirements and protections of the Fourth, Sixth, and First Amendments.[409] If the purpose is to monitor conversations toward understanding a terrorist threat, FISA may be used if its requirements are otherwise met. If both objectives are present, responsible officials should weigh which purpose is dominant and use the appropriate path toward authorized surveillance. The 2001 amendment and its 2006 codification did not tear down the wall; nor did the 1978 purpose language build it. Nor could these phrases in FISA knock down a set of protections that the Constitution requires.

Within a few months of the FISCR decision,[410] the Justice Department reported to the House Judiciary Committee that the procedures approved by the FISCR greatly improved the way that investigations are conducted, in terms of efficiency, order, and effectiveness.[411] Approximately 4500 open intelligence files were shared with criminal prosecutors during that several month period.[412] In 2003, the FBI issued a directive, the Model Counterterrorism Investigations Strategy (MCIS), which requires law enforcement and intelligence investigators to work together as part of the same teams investigating terrorism.[413]

407. Kate Martin & Viet Dinh, *Section 203: Authority to Share Criminal Investigative Information*, *in* PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT 12 (Stewart A. Baker & John Kavanagh eds., 2005) ("Even the most strident opponents of the USA PATRIOT ACT would not want another terrorist attack to occur because law enforcement and intelligence communities were prevented from talking to each other."). This rhetoric obscures the fact that FISA did not prevent such sharing of information. *In re* Sealed Case, 310 F.3d 717, 727 (FISA Ct. Rev. 2002).

408. *See* Banks, *supra* note 16, at 1158 (discussing the focus of the primary purpose provision).

409. *See* Swire, *supra* note 296, at 1361.

410. *In re Sealed Case*, 310 F.3d 717.

411. Letter from Jamie E. Brown, Acting Assistant Att'y Gen., U.S. Dep't of Justice, to F. James Sensenbrenner Jr., Chairman, House Comm. Judiciary 15–16 (May 13, 2003).

412. *Id.* at 16.

413. *See* Dan Eggen, *FBI Applies New Rules to Surveillance*, WASH. POST,

All terrorism investigations are "handled from the outset like an intelligence or espionage investigation," run out of the counter-terrorism division at the FBI, and investigators from the blended teams may use FISA processes.[414] One aim of the new system is to deemphasize criminal prosecution in favor of longer term surveillance, although prosecutors that bring criminal charges will be able to use FISA surveillance at trial.[415]

In September 2005 testimony before the Senate Judiciary Committee, a senior FBI official stated that the Patriot Act, the Ashcroft information sharing procedures, and the FISCR decision "removed real and perceived barriers to coordination" among the FBI and other intelligence agencies.[416] In a September 2006 release the Justice Department reported an increase of more than 122 percent in court-approved FISA applications between 2001 and 2005, with anticipated 10 percent growth for 2006.[417] In addition, since 2004 the Department had reduced the backlog of pending FISA requests by about 60 percent, and reduced the number of days it takes to process FISA requests by 35 percent.[418] The size of the lawyer staff at OIPR was tripled during the same period, and standardized pleadings and automated drafting have made FISA filings shorter and easier to produce.[419]

Former NSA General Counsel Stewart Baker maintained that the wall was born out of fear.[420] Baker believed that agency professionals "were focused on the hypothetical risk to privacy if foreign intelligence and domestic law enforcement were allowed to mix" and on the chance "that years of successful collaboration would end in disaster if the results of a single collaboration could be painted as a privacy scandal."[421] Whatever the motivation, Baker is surely correct that the wall was deeply embedded in the FISA culture when these decisions

Dec. 13, 2003, at A1.

414. *Id.*

415. *Id.*

416. *Able Danger and Intelligence Information Sharing: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 35 (2005) (statement of Gary M. Bald, Executive Assistant Dir., Nat'l Sec. Branch, FBI).

417. DOJ, FACT SHEET, *supra* note 6.

418. *Id.*

419. *Id.*

420. Stewart Baker, *Wall Nuts*, SLATE, Dec. 31, 2003, http://www.slate.com/id/2093344/.

421. *Id.*

were rendered in 2002.[422] The FISC did not see the risk identified by Baker as hypothetical, and it had long experience in managing the FISA process.[423] The FISCR appeared to side with Baker, but it had never seen a FISA application before.[424] If the FISCR decision is forming the basis for implementing FISA now, the FBI is permitted to obtain FISC permission to conduct a secret electronic surveillance or search for the primary purpose of investigating a crime even though there is no probable cause to suspect the commission of a crime.

2. Statutory Obsolescence and Lone Wolf

One by-product of the compromising that was necessary to produce FISA was a set of definitions and procedures that were difficult to understand and apply, even in the beginning.[425] As sometimes happens with major legislation that is complicated at the outset, amendments are made and, over time, what was complex becomes hopelessly complex.

In addition, the investigative resources directed at countering terrorism have grown considerably, and their orientation has shifted. In the years since FISA was implemented, Congress has, often at the behest of the executive branch, criminalized more and more national security and terrorism-related conduct, adding hundreds of new offenses to the federal criminal code.[426] As a result, in the universe of foreign intelligence surveillance, a law enforcement purpose for the surveillance inevitably occupies a larger portion of the whole than it once did. The challenges in sorting out what should be FISA surveillance and what should follow the law enforcement model are greater now than they were in 1978.

As terrorism overtook espionage as the dominant foreign intelligence collection challenge, the foreign power and agent of a foreign power concepts did not align easily with targeting objectives.[427] The growing criminalization of terrorism made the

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

423. Banks, *supra* note 16, at 1167–71.

424. *See id.* at 1171–74.

425. *See* Banks, *supra* note 16, at 1161–62 (describing early difficulties of overlapping procedures); Swire, *supra* note 296, at 1325 (calling FISA a "grand compromise").

426. *See* NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT 5–7 (1st ed. 2005) (listing the major legislative programs).

427. *See* Solove, *supra* note 397, at 1289 (noting that FISA was created for gathering intelligence about foreign powers inside the United States).

minimization rubric for what was collected pursuant to FISA harder to sustain, while the growing need for cooperation and information sharing was not contemplated when FISA was enacted in 1978. Congress never took the initiative, nor did the executive branch, to step back and rewrite FISA from top to bottom. As a result, the issues that have plagued FISA have lingered, and new ones crop up. Amendments have been made piecemeal.

When Congress amended FISA in 2004 to provide authority to conduct FISA-ordered investigations of so-called "lone wolf" terrorist suspects,[428] it was billed by many as "the Moussaoui fix"—referring to the failure to find that Moussaoui was an agent of a foreign power as defined by FISA because he had no apparent links to terrorist organizations.[429] As amended, the "[a]gent of a foreign power" may include any person, other than a United States person, who . . . "engages in international terrorism or activities in preparation therefore."[430] In expanding FISA to reach these unaffiliated persons, or those for whom the foreign agency connection cannot be established by probable cause, Congress did not attempt to revisit its 1978 formula for identifying targets, an approach that was derived from traditional concerns with espionage and counterintelligence.[431] Logically, the foreign agency concept could not bear the weight of the lone wolf amendment in 2004. If an individual may be targeted for FISA surveillance without any showing of a connection to any other supposed terrorists, the idea of "agency" simply does not fit. Congress can call an unaffiliated person an agent, but the Act does not require any agency relationship.

Yet the lone wolf amendment is arguably among the most defensible changes to FISA since 1978. On the one hand, recent terrorist trends suggest that the lone wolf is the terrorist of our time, symbolized by the universal violent jihad rhetoric.[432] In-

428. 50 U.S.C.A. § 1801(b)(1)(C) (West 2006).

429. 9/11 COMMISSION REPORT, *supra* note 167, at 274.

430. 50 U.S.C.A. § 1801(b)(1)(C). Like several other Patriot Act provisions, the lone wolf authority was set to expire at the end of 2005, but in March 2006 Congress extended the sunset date for the lone wolf provision to December 31, 2009. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 103, 120 Stat. 192, 195 (2006) (codified at 50 U.S.C.A § 1801 (West 2006)).

431. *See* Solove, *supra* note 397, at 1289 (noting that FISA was created to combat espionage).

432. *See, e.g.*, Robert S. Mueller, III, Dir., FBI, Remarks at the City Club of Cleveland (June 23, 2006) (transcript available at http://www.fbi

dividual terrorists are not a new phenomenon, and examples of the lone wolf trace back at least as far as European anarchists in the late nineteenth century.[433] As Bob Chesney has explained, internet and encryption technologies have joined with the growing violent jihad movement and the partial success of efforts to curtail violent jihad organizations to facilitate the growth of unaffiliated terrorists and their causes.[434] Conducting surveillance only of those who are foreign agents may miss some of the most important targets.

On the other hand, the extension of FISA processes to unaffiliated individuals does not solve the problem of coming up with sufficient information to meet the FISA probable cause requirement.[435] Put differently, investigators still have to know something about the lone wolf target before they may begin FISA surveillance, and learning that modicum of information is made no easier by the lone wolf amendment.

At first blush, the lone wolf provision may appear to permit intrusive electronic surveillance pursuant to FISA of an especially broad array of individuals[436]—from those who are suspected of buying or selling component materials for weapons of mass destruction to those who make donations to apparently humanitarian organizations in the Middle East.[437] However, the lone wolf provision does not apply to U.S. persons[438] and it requires pursuit of "foreign intelligence" and a connection to "international terrorism," offering protection against targeting

.gov/pressrel/speeches/mueller062306.htm) ("Today, terrorist threats may come from smaller, more loosely-defined individuals and cells . . . who are inspired by a violent jihadist message. These homegrown terrorists may prove to be as dangerous as groups like al Qaeda, if not more so.").

433. PAUL WILKINSON, TERRORISM AND THE LIBERAL STATE 97–99 (2d ed. 1986).

434. Chesney, *supra* note 66, at 439–40, 445.

435. Kim Taiple, *Whispering Wires and the Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, BULL. ON L. & SEC. (Ctr. on Law & Sec., New York, N.Y.), Spring 2006, at 4, 4, 8 n.7.

436. *See* 50 U.S.C.A. § 1801(b)(1)(C) (West 2006) (including "any person" engaging in terrorist activities).

437. *See id.* § 1801(c) (defining international terrorism activities).

438. *Id.* If it is illogical to call a lone wolf an agent of a foreign power, so too does it not make logical sense to exclude U.S. persons from eligibility for lone wolf status under FISA. Homegrown terrorism exists, and that terrorism can spring from domestic as easily as foreign sources. Once foreign agency is eliminated as a real requirement for FISA targeting, the logic of excluding U.S. persons evaporates. Our constitutional system may not permit extending FISA status to domestic lone wolves, but this is a topic for another article.

domestic activities.[439] Yet in the post-September 11 era, where supposed links to al Qaeda are legion, the tendency to rely on FISA to investigate even the most speculative suspicions of a connection to international terrorism by lone wolves could turn FISA surveillance into a quotidian occurrence.

Moreover, there may be a tendency to couple the discretion to conduct electronic surveillance of lone wolves with early arrest and prosecution. If so, cessation of surveillance may impose opportunity costs and a higher likelihood of acquittals than have been the case under the previous foreign agency criteria.[440] With this potential risk in mind, the lone wolf change may be a practical statutory salve to an important policy challenge, while it shows that the original FISA framework for targeting electronic surveillance may not be workable now.

IV. THE FUTURE PROSPECTS

Now that the basic survival of FISA has been called into question, it is important to consider whether FISA can be restored to its useful role in maintaining the security and civil liberties balance. Changes in technology and the dimensions of the modern threat of international terrorism have combined to complicate finding the appropriate mechanisms that may or may not be accommodated inside the FISA scheme. This part of the Article will consider whether technological developments make it impossible for the TSP to be conducted with FISA procedures. Next, the Article will offer some tentative conclusions concerning the lawfulness of the TSP. Then it will evaluate proposed FISA amendments, although in the main they simply relegate FISA to an historic dust bin. Whether the TSP could be reshaped harmoniously with a still-relevant FISA is a hard question, one that I will address briefly in the final two subsections.

A. FISA AND MODERN TECHNOLOGY

When deliberating FISA in 1977, Congress was well aware that NSA had engaged in its share of the abuses chronicled by the Church Committee and others.[441] From 1945 until 1975, NSA received copies of millions of international telegrams sent

439. *Id.* §§ 1801(b)–(c).

440. Chesney, *supra* note 66, at 427.

441. S. REP. NO. 95-604, pt. 1, at 34 n.39 (1977), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3936 (citing S. REP. NO. 94-774, pt. 3, at 733 (1976)).

to, through, or from the United States.[442] NSA intended Operation SHAMROCK to obtain telegrams of foreign targets for foreign intelligence purposes.[443] With the assistance of commercial telegraph companies and without obtaining any kind of judicial warrant, NSA had access to as many as 150,000 telegrams per month, including those of U.S. citizens who were not in any way targeted for foreign intelligence and who reasonably expected their communications to be private.[444] When considering FISA, however, Congress expressly declined to extend FISA procedures to NSA surveillance activities at least in part because of then-recent enhancements in oversight of NSA provided by presidential executive orders and through classified Attorney General procedures.[445] In addition, Congress took note of the "particularly difficult conceptual and technical problems" in regulating NSA, and it opted to leave NSA untouched until separate legislation could be considered.[446]

The modern NSA story is in part about the supposed leapfrogging of technology. The story is familiar. The technologies of surveillance and its evasion change rapidly. The bad guys keep up with them, and the government lags behind, always playing catch up.[447] "NSA does not 'engage in wiretapping'"; its electronic surveillance is referred to as "signals intelligence" or SIGINT.[448] "NSA intercepts entire streams of electronic communications containing millions of calls and e-mails," and screens them through computers that search for key words or phrases, telephone numbers, or Internet addresses.[449] Data that is identified as worthy of further investigation is generated by the computers, and then forwarded to NSA personnel.[450] Of course, the immense volume of electronic communication in the world today is such that NSA collects only a small portion of it. Some of what is collected is in foreign languages, and some is

442. S. REP. NO. 94-774, pt. 3, at 738, 740.

443. *Id.* at 740.

444. *Id.*

445. S. REP. NO. 95-604, pt. 1, at 34 n.40, *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3936; H.R. REP. NO. 95-1283, at 21 (1978).

446. S. REP. NO. 95-701, at 71–72 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 4040–41.

447. *But see* James Bamford, *Big Brother Is Listening*, ATLANTIC MONTHLY, Apr. 2006, at 65, 69 (describing how the NSA attempts to keep up with new technologies).

448. *Id.* at 66.

449. *Id.*

450. *Id.*

encrypted, while technical issues limit the capabilities of NSA computers to find all the desired identified markers.[451] Accordingly, NSA must establish priorities for its collection activities.

Is FISA an impediment to the government in the technology race? One part of the NSA program, first reported by the media in May 2006, apparently consists of collecting meta-data, information about communications, but not the contents of those communications.[452] NSA collects the phone numbers or e-mail addresses and the time and day of communications between sets of numbers or addresses.[453] Computers then sift through the billions of pieces of data and cross reference them with information databases in order to identify persons for further investigation.[454]

The FISA definition of "electronic surveillance" extends to some non-content information, and thus even the indiscriminate data mining program run by NSA may require a FISA application and order before it is performed, or, on an emergency basis, an application within seventy-two hours of approval by the Attorney General.[455] Attorney General Edward Levi testified in 1975 that FISA should include provisions for the approval of "program[s] of surveillance" for foreign intelligence when there are no "specifically predetermined targets" and where "the efficiency of a warrant requirement would be minimal."[456] Of course, Congress enacted FISA without such a provision and the compromise that became FISA included a considered judgment that only individualized consideration of applications for secret surveillance to collect foreign intelligence would be prescribed.

One additional problem with the TSP is that NSA computers do not know who placed the calls or sent the messages, nor do they know the contents of those communications. How

451. *See id.* at 69 ("[The NSA's offices] at Crypto City also houses the nation's largest collection of powerful computers, advanced mathematicians, and skilled language experts.").

452. Leslie Cauley, *NSA Has Massive Database of Americans' Phone* Calls, USA TODAY, May 11, 2006, at 1A; John O'Neil, *Bush Says U.S. Spying Is Not Widespread*, N.Y. TIMES, May 11, 2006, at A1 (describing the program and its description by USA Today).

453. *See* O'Neil, *supra* note 452.

454. *See* Harris, *supra* note 300, at 48.

455. 50 U.S.C. §§ 1801(f), 1805(e), 1805(f)(2) (2000 & Supp. III 2004).

456. 152 CONG. REC. S2340–01 (daily ed. Mar. 16, 2006) (statement of Sen. Specter) (discussing and citing Attorney General Levi's testimony before the Church Committee on U.S. Intelligence Activities).

and based on what criteria does someone demonstrate probable cause or even reasonable suspicion to justify targeted surveillance that triggers FISA? Kim Taipale proposes "the electronic surveillance equivalent of a *Terry*[457] stop"—in this case "an authorized period for follow-up monitoring or investigation of initial suspicion derived from automated monitoring."[458] Taipale's reasonable suspicion standard would form the basis for the judgment either to discontinue or continue the automated monitoring at this early stage. If the monitoring produces probable cause of foreign agency (or lone wolf status), a traditional FISA process could be launched by NSA and the Department of Justice.[459] Taipale does not suggest that programmatic measures be used indiscriminately in search of terrorist activities. Instead, officials should direct these techniques "against known or reasonably suspected foreign terrorist communication sources," sources not subject to FISA or a traditional law enforcement warrant, and employ them to "automate the process of looking for connections, relationships, and patterns for further follow-up investigation."[460] Taipale offers examples—"Abu Musab Zarqawi's cell phone number or a known al Qa'ida communication network in Pakistan, Saudi Arabia, or Hamburg."[461] In a similar vein, Judge Richard Posner laments that, while FISA has value for monitoring known terrorists, "it is hopeless as a framework for detecting terrorists."[462] Posner argues that the FISA requirement of probable cause of foreign agency before electronic surveillance may be approved is of no help "when the desperate need is to find out who is a terrorist."[463] Yet what kind of rule-based program could permit surveillance in the circumstances of concern to Taipale and Judge Posner that would consist of anything other than the unilateral discretion of executive officials and intelligence professionals? Who would determine what counts as a suspected foreign terrorist communication source for these purposes, and what cri-

457. Terry v. Ohio, 392 U.S. 1, 23 (1968) (permitting police to detain a suspect for a reasonable period without probable cause to arrest).

458. Taipale, *supra* note 435, at 1, 5–6.

459. *Id.* at 7.

460. *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the H. Permanent Select Comm. on Intelligence*, 109th Cong. 1–5 (2006) (statement of Kim Taipale, Executive Dir., Ctr. for Advanced Studies in Sci. & Tech. Policy).

461. Taipale, *supra* note 435, at 9 n.15.

462. Posner, *supra* note 336.

463. *Id.*

teria would be used to decide whether and how to continue follow-up investigations?

B. IS THE TSP LAWFUL?

At this writing, a few legal conclusions about the TSP may be at least tentatively drawn. First, the NSA has, by the public admissions of administration officials, conducted the foreign intelligence "electronic surveillance" that is subject to FISA, taking into account the changes in technology since 1978.[464] Second, although the President may have had Commander-in-Chief Clause authority to engage in a range of surveillance activities incident to conducting a lawful war, in the absence of congressional legislation limiting such discretion, the Supreme Court has consistently upheld the authority of Congress to limit that authority.[465] In this context, Congress intended to foreclose the authority the President might have previously had under the Constitution to conduct such surveillance without statutory authority.[466] The same section of FISA also forecloses implying foreign intelligence electronic surveillance authority in any other statute—only a clear authorization in a statute subsequent to FISA could overcome the original preclusion.[467] The administration has argued that the Authorization for the Use of Military Force (AUMF)[468] permits the NSA surveillance, extrapolating from the Supreme Court's determination that the AUMF authorized the use of military detention in *Hamdi v. Rumsfeld*.[469] The AUMF argument could fail on the context distinctions between detention of those captured on a battlefield and electronic surveillance of Americans inside the United States. The distinctions matter less, however, than the stark history of the immediate post-September 11 period. At the same time that Congress passed the AUMF, it was considering versions of what later became the Patriot Act. Among the most

464. 50 U.S.C. § 1801(f)(1),(2) (2000 & Supp. III 2004); *see* Gonzales, Georgetown Remarks, *supra* note 316.

465. *See* Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2775 (2006); Rasul v. Bush, 542 U.S. 466, 473–74, 485 (2004); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585–89 (1952); Little v. Barreme, 6 U.S. (2 Cranch) 170, 178–79 (1804).

466. 18 U.S.C. § 2511(2)(f) (2000 & Supp. III 2004).

467. *See* Banks *supra* note 16, at 1153–58.

468. Authorization of Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

469. Hamdi v. Rumsfeld, 542 U.S. 507, 518 (2004) (plurality opinion); *id.* at 587 (Thomas, J., dissenting).

important features of the Patriot Act were those that amended FISA to provide greater tools for the government in the war on terrorism.[470] It is difficult to conclude that the AUMF permitted electronic surveillance inside the United States beyond what Congress was simultaneously revising in FISA. Apart from its questionable application to electronic surveillance inside the United States, the AUMF should not be read to overcome the "exclusivity" provision of FISA. The comprehensiveness of FISA is reinforced by the section that permits electronic surveillance without approval by the FISC for fifteen days immediately following a declaration of war.[471]

The stronger constitutional argument for the administration is that Article II permits the President to authorize warrantless surveillance of Americans inside the United States to gather information about terrorist activities.[472] Two courts of appeal so held before FISA was enacted.[473] Now, however, the constitutional question is whether FISA is unconstitutional in restricting the President's authority to authorize warrantless surveillance.[474] Congress enacted FISA pursuant to its Commerce Clause authority to regulate wire communications between states and between nations.[475] FISA is also an exercise of the Necessary and Proper Clause, because it serves to "carry[] into execution" other national security powers of Congress and also because it reaches NSA (part of the Department of Defense) incident to its power "[t]o make Rules for the Govern-

470. Patriot Act, Pub. L. No. 107-56, §§ 201–202, 115 Stat. 272, 278 (2001) (amending 18 U.S.C. § 2516(1) (2000)) (expanding law enforcement surveillance authorities to reach terrorism-related activities); *id.* §§ 203(b), (c), 115 Stat. 272, 280–81 (amending 18 U.S.C. § 2510, 50 U.S.C. § 403-5d (2000)) (authorizing information sharing between law enforcement and intelligence agencies); *id.* § 206, 115 Stat. 272, 282 (amending 50 U.S.C. § 1805 (2000)) (authorizing roving wiretaps); *id.* §§ 209, 210, 212, 115 Stat. 272, 283–86 (amending 18 U.S.C. §§ 2510, 2702, 2703 (2000)) (allowing access to wire and electronic communications); *id.* §§ 214, 215, 115 Stat. 272, 286–88 (amending 50 U.S.C. §§ 1842, 1843, 1861, 1862 (2000)) (limiting pen register and trap and trace authority and access to business records of United States persons); *id.* § 218, 115 Stat. 272, 291 (amending 50 U.S.C. § 1804 (2000)) (change in the purpose standard).

471. 50 U.S.C.A. § 1811 (West 2006).

472. *See* U.S. CONST. art. II, § 2, cl. 1.

473. United States v. Butenko, 494 F.2d 593, 605–08 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).

474. *See* Statement of David S. Kris, *supra* note 313 (applying the separation of powers balancing and concluding that "a lot turns on the facts").

475. U.S. CONST. art. I., § 8, cl. 3.

ment and Regulation of the land and naval Forces."[476] Does FISA unconstitutionally restrict the President's national security authority? The answer turns on the facts of the TSP, which are not publicly available. If General Hayden describes the program accurately, the administration made a stark choice to circumvent the FISA probable cause and judicial approval processes for a lower threshold without judicial involvement. Unless something less than probable cause to believe that the target is a foreign agent is demanded because of changes in surveillance technology, existing judicial precedent would not support the TSP.[477]

In the wake of the revelations of the TSP, instead of chastising the administration for acting outside an inter-branch system for implementing one of the most important national security measures of our time, Congress may be on the brink of gutting what remains of the FISA system.

C. PROPOSALS TO AMEND FISA

Most of the proposals to amend FISA generated after the TSP story broke would make radical changes in the law. The bills favored by the administration would repeal the FISA exclusivity provision and its attendant criminal penalties, thus making it optional for the administration to seek an order from the FISC for electronic surveillance inside the United States against United States persons.[478] This is, of course, the heart of the 1978 compromise—subjecting electronic surveillance to the terms of the FISA deal in every instance.[479] Between FISA's enactment in 1978 and September 11, Attorneys General issued forty seven emergency authorizations under FISA.[480] In the first eighteen months after September 11, the Attorney General authorized more than 170 emergency authorizations

476. *Id.* art. I, § 8, cl. 14.

477. *See* Banks *supra* note 16, at 1181–84.

478. *See* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., TERRORIST SURVEILLANCE ACT OF 2006: S. 3931 AND TITLE II OF S. 3929, THE TERRORIST TRACKING, IDENTIFICATION AND PROSECUTION ACT OF 2006 at 8–9 (2006).

479. *See* Statement of Former National Security Officials, Sept. 25, 2006, http://www.cdt.org/security/20060927officials.pdf (expressing opposition to proposal to eliminate the exclusivity provision of FISA and signed by former FBI Directors and Counsel, former CIA Counsel, Department of Justice officials).

480. Dan Eggen & Robert O'Harrow, Jr., *U.S. Steps Up Secret Surveillance*, WASH. POST, Mar. 24, 2003, at A7.

for electronic surveillance or search.[481] To provide an explicit escape from FISA for the executive branch would likely curtail significantly the FISC oversight that emergency applications currently receive.

Despite General Hayden's claims that the TSP is narrowly focused on targets that are reasonably suspected of terrorist links and is not a drag net or massive data mining program, proposals were made to amend FISA to authorize "programmatic approvals of cutting-edge technologies—including automated monitoring of suspected terrorist communications."[482] Kim Taipale argues that FISA should be amended so that its definition of "electronic surveillance" can accommodate orders to capture the data and voice communications inside modern networks.[483] He also acknowledges that the automated monitoring that Hayden favors could not be done under FISA as it now stands because the intercepts would not meet the probable cause standard, even if submitted retroactively under the emergency authority.[484]

The administration-backed proposals to amend FISA would ratify the TSP by authorizing the FISC to approve "electronic surveillance programs" inside the United States, for up to ninety days, renewable by the FISC.[485] Such a program would have as a "significant purpose the gathering of foreign intelligence information or protecting against international terrorism" where it is "not feasible" to name the targets or locations, where "flexibility" is required for "effective" surveillance, and where an "extended period" of surveillance is contemplated.[486] The FISC could authorize a program for up to 90 days initially, and the court could reauthorize a program for any "reasonable" period.[487] If the FISC denied an application, the Attorney General could reapply or appeal to the FISCR.[488] If, during an approved program of surveillance, the Attorney General determines that any target of the program could satisfy the criteria for individualized consideration under FISA, surveillance of that target must be discontinued unless an ap-

481. *Id.*
482. Taipale & Carafano, *supra* note 336.
483. Taipale, *supra* note 435, at 5–7.
484. *Id.* at 8 n.9.
485. BAZAN, *supra* note 478, at 12–13.
486. *Id.*
487. *Id.*
488. *Id.*

plication is made, either for continued programmatic surveillance or for an individual order of surveillance from the FISC.[489]

So styled, this proposal is just as devastating to FISA as the repeal of the exclusivity provision. The "program" could be used when its sole purpose is the collection of evidence for prosecution, and, instead of any version of a probable cause requirement, the program has only to be "reasonably designed" to meet its objectives.[490] The "electronic surveillance program" could become the contemporary general warrant, going beyond even what has been publicly described as the TSP.

The administration-backed proposals also expand the definition of "agent of a foreign power" to reach non-U.S. persons who possess, control, transmit, or receive significant foreign intelligence information while in the United States.[491] This definition requires no connection of the target to a terrorist organization and no showing of a link to international terrorism. Both approaches end the collaborative roles of Congress and the judiciary in monitoring intrusive surveillance for foreign intelligence inside the United States, and both restore constitutional doubt to one of the administration's most important counters to the threat of terrorism.

One of the main choke points in FISA is the expansive definition of "electronic surveillance."[492] Whether by prescient drafting or simple luck, the definition is broad enough to reach modern communications technologies, including many of the technologies that NSA uses. To avoid becoming ensnared in traditional FISA procedures, the 2006 bills the administration favors would narrow the previously expansive definition, enabling NSA electronic monitoring or data mining so long as the government is not intentionally targeting a United States person inside the United States.[493] No order of the FISC would be required in these situations, including the vast vacuum cleaner-like operations of NSA.[494] Warrantless surveillance would be expressly permitted under these bills, including any communication between a U.S. person and foreign power or agent of foreign power, so long as the target is one of the latter

489. *Id.* at 3.
490. *Id.* at 6 n.9.
491. *Id.* at 9–10.
492. 50 U.S.C. § 1801(f) (2000 & Supp. 2004).
493. BAZAN, *supra* note 478, at 10–11.
494. *Id.* at 12–15.

categories.[495] Existing minimization requirements would also be eliminated, so that the contents of electronic communications of U.S. persons could be stored and disseminated without statutory restriction.[496]

A more modest set of proposals seeks to retain the FISA compromise, update some provisions in light of changing technologies, and assure that the Justice Department has adequate resources and personnel to meet the challenges of the FISA processes.[497] One bill would extend the FISA emergency period from seventy two hours to seven days and allow the Attorney General to delegate the authority to approve FISA applications and to authorize emergency surveillance.[498] This bill would also require development of improved management systems for facilitating the FISA application process and authorize hiring more staff to meet the demands of regular or emergency applications under FISA.[499] While these measures may stand the least chance of enactment in the short term, their enactment could actually restore some elements of the FISA compromise.

As described by Attorney General Gonzales and General Hayden, the TSP targets communications involving those for whom there is reasonable suspicion of a link to al Qaeda or a group of affiliates of al Qaeda.[500] Monitoring occurs then only if one end of the communication is abroad.[501] Although this warrantless electronic surveillance itself violates FISA, the leading bills would ratify the TSP and then go farther and permit the twenty-first century equivalents of general warrants.[502] Viewed in the aggregate, the bills would authorize NSA to listen in on the contents of phone conversations of U.S. citizens inside the United States without probable cause or even reasonable suspicion (the "program" must be "reasonably designed" to intercept the communications of suspected terrorists) that the person is connected in any way to terrorism—even where the conversation itself has nothing to do with terrorism (interception permitted of a person who "is reasonably believed to have commu-

495. *Id.*

496. *Id.* at 11–12.

497. Foreign Intelligence Surveillance Oversight and Resource Enhancement Act of 2006, S. 4051, 109th Cong. (2d Sess. 2006).

498. *Id.* § 201.

499. *See id.* § 102.

500. *See* Press Briefing, Gonzales & Hayden, *supra* note 322.

501. *Id.*

502. *See* BAZAN *supra* note 478, at 12–13.

nication with or be associated with" a suspected terrorist).[503] Because the purpose of the warrantless surveillance program may be to "protect against international terrorism," it could be employed when the sole objective is to build evidence for prosecution.[504] In other words, the bills permit wholesale eavesdropping.

D. CAN FISA BE SAVED?

It is difficult from this vantage point—thirty years out—to understand that FISA may have been the best possible accommodation of the conflict between national security and civil liberties when it comes to surveillance. It is unrealistic to expect a model like FISA to last forever or for it to remain immune from the need for revisions and updates. Congress first amended FISA in 1994, when it added physical search authority through several provisions that set up parallel processes to those in place for electronic surveillance.[505] Pen register, trap and trace, and business records acquisition were added to the FISA processes in 1998,[506] while less extensive revisions were made to the definition of "agent of a foreign power" in 1999 and to targeting language in 2000.[507]

The 2001 Patriot Act did more than change the foreign intelligence "purpose" requirement in seeking to increase the sharing of intelligence and law enforcement information. In more ways than one, the Patriot Act foretold the death of FISA. In the emergency atmosphere that engulfed Congress after September 11, a hastily considered set of fundamental changes to FISA was enacted, buffered by the fact that many were subject to a four-year sunset.[508] Although the "significant purpose" amendment was chosen for more extensive consideration in this Article, the theme developed here could have been

503. *Id.* at 6 n.9.

504. *See id.* at 3.

505. Counterintelligence and Security Enhancements Act of 1994, Pub. L. No. 103-359, 108 Stat. 3423 (2001).

506. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396 (1998).

507. Intelligence Authorization Act for Fiscal Year 2001, Pub. L. No. 106-567, § 602, 114 Stat. 2831, 2851–53 (2000); Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, § 601, 113 Stat. 1606, 1619 (1999).

508. Patriot Act, Pub. L. No. 107-56, § 224(a), 115 Stat. 272, 295 (2001); *see, e.g.*, Patricia Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 429 n.31 (2005) (describing FISA's sunset provisions).

sketched using the roving wiretaps provision,[509] the enhanced pen register and trap and trace authorities,[510] or the expansion of the national security letters and document production authorities to reach "any tangible thing."[511]

After a modest expansion of information sharing authority in FISA by the Homeland Security Act of 2002,[512] the 2004 intelligence reform legislation significantly expanded FISA by adding the "lone wolf" amendment to "agent of a foreign power."[513] As the sunsets loomed in 2005, Congress approved short-term extensions until enacting the USA PATRIOT Reauthorization Act of 2005 in March 2006.[514] Fourteen of the sixteen provisions due to sunset were made permanent in the Act, while the roving wiretaps, "tangible thing," and "lone wolf" provisions were extended until the end of 2009.[515]

Even if Congress enacts none of the proposals to amend FISA being considered at the end of the 109th Congress, it is fair to say that the compromise collapsed with September 11. Perhaps the richest example of how the emergency atmospherics worked to undo the compromise that served well for more than two decades is the review of the Patriot Act purpose change by the FISC and the FISCR. At the time, that group of seven FISC judges probably understood FISA mechanics, processes, and the delicate balancing of interests it represented better than anyone. In the face of the emergency and the statutory change, the judges did their best to preserve the central purpose of FISA while respecting the changes made in the Patriot Act. The FISC opinion reached a fair accommodation of the competing interests, even though the court's emphasis on complying with the minimization requirements of FISA struck many readers, including the FISCR, as not responsive to the government's argument and not as central to their outcome as the original purposes of FISA and its reasonableness in light of the Fourth Amendment.

509. Patriot Act, § 206.

510. *Id.* § 214.

511. *Id.* §§ 215, 505; *see* Schulhofer *supra* note 163, at 544–61.

512. Homeland Security Act of 2002, Pub. L. No. 107-296, § 898, 116 Stat. 2258 (2002) (amending 50 U.S.C. § 1806(k)(1)).

513. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C.A. § 1801(b)(1)(c) (West 2006)).

514. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006).

515. *Id.* § 103, 120 Stat. 195 (2006).

Minimization procedures are designed to protect U.S. persons from having what would typically be the inevitable by-product of indiscriminate electronic surveillance—communications intercepted that are not foreign intelligence—from being acquired, retained, or disseminated.[516] As the FISC saw a FISA future under the proposed OIPR procedures, the amount of non-foreign intelligence information that would be collected would increase, and the possibility of direction and control of a FISA investigation by the Criminal Division meant that considerable non-foreign intelligence information would be collected, stored, and disseminated.[517] In effect, the FISC worried that FISA would be used to enforce the criminal law, and that application of FISA surveillance would be inconsistent with the underlying purpose of minimization.[518]

Based on the long experience of the FISC judges in working with FISA and its implementation, their concern with the effects of the new procedures on minimization was understandable. Particularly since the 1995 procedures promulgated by Attorney General Reno heightened the sensitivities of FISC judges to inappropriate uses of FISA in criminal investigations, the court was especially wary of endorsing what could be seen as a way to work around the rigors of Title III warrants.[519] Yet the FISC was, to some extent, a prisoner of its limited perspective and its symbiotic relationship with OIPR. Without meaningful oversight by Congress or other Article III courts, the FISC was "coached" by OIPR after 1995 to elevate the wall and information screening procedures beyond the statutory requirements.[520] FISA explained the prohibition on the Criminal Division directing or controlling FISA surveillance, but it did not justify the restrictive screening walls that stood in the way of effective cooperation and coordination. Thus, the 2002 FISC decision puzzled many observers. If the proposed OIPR procedures would enable prosecutors to use FISA when obtaining Title III warrants was too difficult, the more visible and concrete legal problem was that the purpose of the investigation was no

516. *In re* Sealed Case, 310 F.3d 717, 737 (FISA Ct. Rev. 2002).

517. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624–25 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

518. *Id.*

519. *Id.* at 619–24.

520. *See* 9/11 COMMISSION REPORT, *supra* note 167, at 78.

longer to collect foreign intelligence, or that the surveillance would be undertaken in violation of the Fourth Amendment.

It was understandable for the FISCR to rebuke the FISC for basing their decision on the FISA minimization requirements, and for failing to respond directly to the Patriot Act arguments advanced by the government. As the FISCR construed FISA, the minimization requirements allow the dissemination for law enforcement purposes of non-foreign intelligence information that is evidence of ordinary crimes.[521] In addition, the FISCR correctly noted that expanding foreign intelligence collection to include evidence of crimes is not the same as directing a FISA investigation for the purpose of building a criminal case.[522] In addition, the "chaperone requirement" that the FISC fashioned and the FISCR overturned,[523] where OIPR was to "be invited" to all meetings between the intelligence and criminal division staff, was cumbersome and not essential to the preservation of the foreign intelligence essence of FISA.

Still, it was not "quite puzzling," as the FISCR proclaimed, that the pre-Patriot Act Justice Department read FISA "as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents—even for foreign intelligence crimes."[524] As noted above, the FISCR conflated what FISA surveillance is used for with the purpose for seeking FISA procedures. Even though the foreign agency definition is, as the FISCR noted, "grounded on criminal conduct."[525] That OIPR misconstrued the procedures and applied them in a skewed fashion to erect barriers to sharing information is highly unfortunate, but it is not a justification for eliminating the central protection against law enforcement direction and control of the FISA processes. FISA requires a significant foreign intelligence purpose before surveillance may be approved by the FISC. It was that assurance that the FISC was understandably seeking to protect.

In any case, reversal of the FISC was an overreaction, and the rhetoric of crisis and fear appeared to outstrip calm reflection in its opinion. In their first ever consideration of a FISA matter, the three judges misunderstood the historical distinctions about primary purpose that FISA case law created. The

521. 50 U.S.C. § 1801(h)(3) (2000); *In re Sealed Case*, 310 F.3d at 736.
522. *In re Sealed Case*, 310 F.3d at 735–36.
523. *Id.* at 720.
524. *Id.* at 723.
525. *Id.*

FISCR also misidentified the source of the information-sharing problem—the cultures and traditions of intelligence and law enforcement, not FISA—and, in doing so, overturned a thoughtful effort by the full and experienced FISC to preserve the fundamental FISA values. By suggesting that there may be constitutional problems with FISA in hamstringing executive power if it were read as the FISC interpreted it,[526] the FISCR drove a stake at the heart of the FISA compromise, while failing to stop the Justice Department from unraveling one of the principal understandings that helped build FISA in the beginning.

The FISCR reasonably feared that it may be impossible to separate the criminal conspiracy from the terrorist activities elements of a foreign organization.[527] Yet the court gave too little credit to the tendency of potential abuses of the secret FISA authorities. While the need to share information and even to combine law enforcement and intelligence investigative teams may be reasonable, it does not follow that the Ashcroft guidelines option of having the criminal team initiate, direct, and control a FISA investigation is justified.[528]

Ironically, the differences between the pre- and post-Patriot Act versions of FISA were not that great, at least not regarding the purpose requirement.[529] Most of the time it will be possible to ascribe a "significant" foreign intelligence purpose in making an application to the FISC where the government is also developing a criminal case.[530] The differences between the 1995 FISC guidelines, (as written, not as applied) and what the Justice Department proposed in 2002 would likely matter in only a few instances.[531] Following the current counter-terrorism prevention paradigm, the government may decide to break up what it believes to be a terrorist conspiracy by prosecuting a collateral crime, such as immigration violations or credit card fraud. If the criminal evidence is collected during FISA surveillance, may it be used to prosecute, even though the crimes are unrelated to the foreign intelligence or counter-terrorism purpose of the surveillance? Most of the time

526. *Id.* at 731.

527. *Id.* at 736.

528. *See* Schulhofer, *supra* note 163, at 540.

529. Banks, *supra* note 16, at 1177–81.

530. *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process*, *Hearing Before the S. Judiciary Comm.*, 107th Cong. 126 (2002) (statement of David S. Kris, Associate Deputy Att'y Gen.).

531. Banks, *supra* note 16, at 1191.

the collateral crime—credit card fraud, for example—will be connected to the terrorist activities and will thus present an easy "significant purpose" determination in the FISA certification. If, however, the strategy at the time the FISA application is made is to find the evidence of crimes unrelated to the foreign intelligence—a suspected terrorist who consumes child pornography, for example—FISA should not be available for the surveillance because the law enforcement and foreign intelligence interests are not intertwined, and the enforcement procedures should be available for investigation and prosecution of the crimes. If some unrelated collateral crimes are discovered later, during FISC-approved foreign intelligence collection, then the criminal evidence should be available in a prosecution. Although a "significant" foreign intelligence purpose is present in both examples, the purpose of the FISA processes would be subverted if the unrelated collateral crimes strategy is allowed to direct and control FISA surveillance.

1. Minimization Reforms?

Consistent with the prevention strategy, it would be possible to amend the minimization requirements in FISA to permit more real time information sharing between foreign intelligence and law enforcement investigators. As FISA minimization is now prescribed, criminal evidence obtained through FISA procedures disseminated for law enforcement purposes is evidence of a crime "which has been, is being, or is about to be committed."[532] Minimization thus requires that responsible officials make an a priori or contemporaneous decision that the collected information is evidence of a crime. The *Sarkissian*, *Duggan*, *Hammoud*, and *Lakhani* examples in the introduction to this Article are model applications of permissible sharing of law enforcement information consistent with the minimization requirements.[533] In *Sarkissian, Duggan,* and *Lakhani*, the collection of foreign intelligence led to the evidence of the crimes.[534] Once the crimes were discovered, the FISA surveillance came to an end. In *Hammoud*, the cigarette smuggling and support for Hezbollah investigations overlapped, but the FISA surveillance was reviewed by the courts and was found to

532. 50 U.S.C. § 1801(h)(3) (2000).

533. *See supra* text accompanying notes 42–55.

534. *See supra* text accompanying notes 42–55.

be undertaken for the primary purpose of collecting foreign intelligence.[535]

In other situations, investigators might not know the intelligence or law enforcement value of collected information at the time it is collected. Investigators may wish to continue collecting foreign intelligence with FISA procedures while at the same time continuing to collect what may amount to evidence of a collateral crime—not a national security crime—and the minimization rule would not permit the sharing of that information with law enforcement. Simply requiring that officials seek a Title III warrant at that point in an investigation may not be a practical option if the result would be to blow the cover off the FISA collection, through delayed notice to the target. Professor Yoo argues that surveillance should be permitted "where there is a reasonable chance that terrorists will appear, or communicate, even if we do not know their specific identities."[536] Yoo offers an example:

> What if we knew that there was a 50 percent chance that terrorist would use a certain communications pipeline, like e-mail accounts on a popular Pakistani service, but that most of the communications on that channel would not be linked to terrorism? A FISA-based approach would prevent computers from searching through that channel for the keywords or names that might suggest terrorist communications, because we would have no specific al Qaeda suspects, and thus no probable cause. Rather than individualized suspicion, searching for terrorists will depend on playing the probabilities, just as roadblocks or airport screenings do.[537]

Professor Yoo maintains that "[i]ndividualized suspicion does not make sense when the purpose of intelligence is to take action, such as killing or capturing members of the enemy."[538] Would Professor Yoo extend this model to electronic surveillance inside the United States? Under his model, are targets of foreign intelligence surveillance "members of the enemy"? Professor Yoo might endorse Kim Taipale's suggestion of an electronic *Terry* stop as a means of accommodating the interest in individualized suspicion.[539] However, if Yoo's premise is accepted, who decides when to forego individualized suspicion, what criteria guide such a decision, and what should be done

535. United States v. Hammoud, 381 F.3d 316, 333–34 (4th Cir. 2004) (en banc), *vacated*, 543 U.S. 1097 (2005).

536. YOO, *supra* note 206, at 111–12.

537. *Id.* at 112.

538. *Id.*

539. *See supra* text accompanying notes 457–71.

with the collected intelligence? Is the inevitable high rate of false positives and accompanying chilling of protected expression and individual privacy worth the gain in surveillance discretion?[540]

2. An Exclusionary Rule for FISA?

Alternatively, minimization could be better managed by the FISC if the federal courts were to enforce a species of exclusionary rule, where the government would be prevented from using FISA-obtained information as evidence in a prosecution of a target for a so-called collateral crime—one having nothing to do with terrorism or national security—if none of the evidence demonstrated that the criminal conduct had any connection to terrorism or national security.[541] If this form of use limit were faithfully observed and enforced, the damage done to the purpose rule by the Patriot Act and the FISCR decision could be repaired, after the fact. Instead of the ex ante purpose rule, the use limit would accomplish the same end ex post.[542] The potential for privacy invasions by investigators using FISA inappropriately would remain, but a check on the utility of the misuse would discourage the original invasion.[543] Elsewhere I proposed the hypothetical of "an international terrorist [who] is also a drug dealer—not to support terrorist activities but to support himself."[544] If FISA surveillance is obtained and evidence of the drug dealing derived from the FISA surveillance is offered as evidence, it should be excluded under this approach, while the same material would be admissible if the target is charged with using his narcotics proceeds to materially support terrorism. In addition, a use limit would, unlike FISA minimization, be based on Fourth Amendment reasonableness and not on the terms of FISA, thus enabling the protections of the use limit to be enjoyed by targets who are not U.S. persons.[545]

540. A full consideration of these issues is beyond the scope of this Article. They are explored generally in MCMAHON, *supra* note 37, *passim*. *See also* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 *passim* (2002).

541. *See* Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61, 102–03 (2006) (proposing such a rule, using the sale of narcotics as an example of the unrelated charge).

542. *Id.* at 103.

543. *Id.*

544. Banks, *supra* note 16, at 1179.

545. Hall, *supra* note 541, at 109.

If some sort of ex post use limit is employed to lessen the minimization task and shore up the weakened purpose requirement in FISA, would the cure be worse than the disease, i.e., would the use limit stand in the way of effective national security or counter-terrorism investigations that do not result in criminal prosecutions? For example, if FISA surveillance uncovers information ultimately insufficient to build a criminal case related to terrorism, but obtains enough information to deport the target for a visa overstay or to prosecute for an unrelated crime, the target might raise the use limit in an eventual deportation hearing or criminal proceeding through the ex parte, in camera hearing to suppress the evidence. Conceivably, the executive could be forced to expose intelligence sources and methods, or simply to alert the target to the nature of the FISA investigation. These are not trivial concerns, but their resolution, if a use limit were accepted and utilized, would likely parallel the outcomes of challenges by criminal defendants under the pre-Patriot Act primary purpose standard—the courts uniformly upheld the FISA surveillance with a high level of deference to the executive branch and the FISC.[546]

3. Improved Oversight of FISA Activities

Because Congress and the courts have not provided meaningful oversight of FISA activities, the FISC has served an important oversight capacity in addition to its responsibility to review applications for surveillance. In 2000, the FISC complained that several applications to the court contained factual inaccuracies.[547] Thereafter, the FBI developed FISA verification procedures to better ensure the accuracy of the facts in each FISA application, particularly those concerning the probable cause determination, and the existence and nature of any parallel law enforcement processes or prior or ongoing asset relationship involving the target. The procedures require computer database searches and efforts to check the status of the target with other units of the FBI.[548] When FOIA requests

546. *Id.* at 110.

547. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620–21 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

548. Memorandum from Michael J. Woods, FBI Office of Gen. Counsel, on Foreign Intelligence Surveillance Act Procedures to Ensure Accuracy of All Field Offices (April 5, 2001), *available at* http://www.fas.org/irp/agency/doj/fisa/woods.pdf.

turned up additional data two years later, the FBI detailed over one hundred instances over two years where procedural requirements of FISA may not have been met, such as conducting wiretaps that were broader in scope and longer in duration than approved by the FISC.[549] This recent record reinforces the importance that Congress should attach to oversight of the FISA processes. Whether Congress provides greater oversight itself or through the FISC, it should not be left to the discretion of the Department of Justice to decide whether and how to use the FISA processes.[550]

E. REVISIONS TO FISA TO ACCOMMODATE THE TSP

During a September 15, 2006 news conference, President Bush commented on the bills in Congress that would amend FISA to account for the NSA surveillance program. One questioner asked about the "eavesdropping program." The President responded: "[Y]es, the illegal eavesdropping program you wanted to call it . . . IEP, as opposed to TSP."[551]

To those who doubt that the technology-challenged Congress is capable of legislating an effective system for surveillance of would-be terrorists, recall that the Bush administration specifically stated in 2001 that the Patriot Act allowed "surveillance of all communications used by terrorists," and that the Act makes us able to "better meet the technological challenges posed by this proliferation of communications technology."[552] In March 2006, when the Patriot reauthorization was completed and most of the sunsets repealed, the Justice Department reiterated that the Patriot Act provisions "brought the federal government's ability to investigate . . . into the modern era—by modifying our investigative tools to reflect modern technologies."[553] So far as all but a handful of members

549. Eric Lichtblau, *Justice Dept. Report Cites Intelligence-Rule Violations by F.B.I.*, N.Y. TIMES, Mar. 9, 2006, at A21.

550. *See* Schulhofer, *supra* note 163, at 541–42 (urging greater FISA oversight of individual cases by FISC judges as well as public and congressional oversight).

551. President's News Conference, 42 WEEKLY COMP. PRES. DOC. 1617 (Sept. 15, 2006).

552. Remarks on Signing of the USA PATRIOT ACT of 2001, 2 PUB. PAPERS 1307 (Oct. 26, 2001).

553. U.S. DEP'T OF JUSTICE, FACT SHEET: USA PATRIOT ACT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005, No. 06-113 (Mar. 2, 2006), *available at* http://www.usdoj.gov/opa/pr/2006/March/06_opa_113.html.

of Congress knew, it had met the technological demands of the executive branch for effective surveillance authorities.

Nonetheless, some variant of the TSP program could be accommodated after changes to FISA that would not rip apart the fabric of the Act. First, FISA could be amended to permit surveillance from "within the United States" of the electronic communications of an agent of a foreign power abroad who is talking to a U.S. person. Modern communications packets of foreign-to-foreign calls or e-mails of non-U.S. persons may pass through the United States as a function of the way that technology operates.[554] The revelation that NSA has been doing just that in the TSP, with the cooperation of telecommunications providers, lets those who we might intercept know something about U.S. capabilities that probably was not known—that even wholly foreign communications may pass through massive switches in the U.S. network. Even though the element of surprise has been eliminated, the location of the switch where the interception of electronic communication by an agent of a foreign power takes place should not affect its legality.

Second, in situations where the government is targeting the foreign communications of a non-U.S. person abroad, FISA does not apply, but if the target calls the United States, the surveillance must be turned off. While amending FISA to exclude from its coverage such surveillance when incident to an ongoing electronic surveillance of a non-U.S. person abroad means that an agency could listen in on innocent persons inside the United States,[555] such a risk might be small in return for the gain to the overall foreign intelligence gained in the surveillance.

Third, the FISA minimization requirements could be made more flexible. The fact that the FISC and FISCR had fundamentally different conceptions of what minimization was designed to accomplish in FISA may be reason enough to revisit its objectives. More important, minimization should take into account the contemporary reality that the information collected cannot always be pigeonholed a priori in a binary world as foreign intelligence or criminal violation evidence. Assuming continued government interest in prosecuting terrorism conspira-

554. Taipale, *supra* note 435, at 4.

555. *See Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA), Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 38–39 (2006) (statement of James X. Dempsey, Policy Dir., Ctr. for Democracy and Tech.).

cies that are inchoate,[556] a FISA investigation that happens to turn up collateral crimes—where seeking a Title III warrant is not a practical alternative in the midst of foreign intelligence collection—could incorporate minimization procedures that are more flexible in terms of the timing of the acquisition, retention, and dissemination of law enforcement information. A twenty-first century FISA might tolerate a looser minimization procedure, with review and oversight mechanisms.

Fourth, in the FISA emergency procedures, one objection made by the Bush administration in defending the TSP was that the FISA procedures required that applications and supporting material for every instance of FISA targeting had to be completed before initiating the surveillance, even though the FISC approval process could wait seventy two hours. The FISA procedures could be streamlined to accommodate the need for speed and efficiency. A senior official could be made responsible for asserting a good-faith belief that the FISA targeting criteria exist regarding the targets in question. The emergency authority would expire, as it now does, at the end of seventy-two hours or when it has been determined by the Attorney General or the FISC that the FISA requirements have not been met.[557]

Of course, traditional judicial review of the TSP may yet invalidate the program as a violation of the Fourth Amendment or FISA. If FISA is not amended to authorize or ratify the TSP in some fashion, a court should enjoin the program as a FISA violation. In the alternative, warrantless electronic surveillance of United States citizens inside the United States constitutes a clear Fourth Amendment violation. One problem in litigating the TSP is that it is impossible to know, without access to classified information, whether the program engages in such surveillance. Based on the statements of General Hayden and Attorney General Gonzales, however, it appears that NSA listens in on the contents of phone and e-mail communications where one participant may be a U.S. citizen inside the United States. If so, the only Fourth Amendment doctrine that could conceivably justify the program is the so-called "special needs" doctrine, excepting from the warrant and probable cause requirements

556. *See generally* Chesney, *supra* note 66 (discussing the continuum of inchoate terrorism conduct that may be prosecuted).

557. The Justice Department reported considerable progress in streamlining the FISA application and review processes, and in reducing the time needed to obtain FISC review in its September 2006 news release. DOJ, FACT SHEET, *supra* note 6.

in situations where the government has "special needs" above and beyond ordinary law enforcement. As has been argued elsewhere, the special needs cases have sustained drunk-driving checkpoints and drug testing in schools, programs that are standardized and relatively non-intrusive.[558] But the doctrine has never supported the highly discretionary and intrusive likes of the TSP. When the FISCR relied on the "special needs" cases to support the Ashcroft procedures lowering the wall,[559] the judges did so in the context of a system that is based on individualized suspicion and prior judicial approval. TSP contains neither protection.

In the first decision to reach the merits of the TSP, Judge Anna Diggs Taylor ruled that the TSP violates FISA, the separation of powers, and the First and Fourth Amendments.[560] Although the analysis in Judge Taylor's opinion was spare, and the case is on appeal,[561] several other pending cases[562] may eventually produce a Supreme Court decision on the TSP.

CONCLUSION

So much of the post-September 11 redirection of our counter-terrorism law and policy in the United States has been based on the impassioned rhetoric of the war on terrorism. Often forsaking reasoned analysis, careful consideration of costs and benefits, and alternative courses of action, our post-September 11 laws and policies have been developed with a sort of bunker mentality, designed to anticipate worst case outcomes. Consider the statement of Vice President Richard Cheney, commenting in the wake of the revelations that a Paki-

558. *See, e.g.*, Letter from Former Government Officials and Law Professors, 10 (Feb. 2, 2006) (replying to DOJ Memorandum), *available at* http://www.cdt.org/security/nsa/20060202scholars.pdf.

559. *In re* Sealed Case, 310 F.3d 717, 745–46 (FISA Ct. Rev. 2002).

560. ACLU v. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006).

561. ACLU v. NSA, 467 F.3d 590, 591 (6th Cir. 2006) (granting motion for a stay pending appeal).

562. *See, e.g.*, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (denying motion to dismiss, holding suit not barred categorically by the state secrets privilege); Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 918–20 (N.D. Ill. 2006) (holding that state secrets privilege barred discovery and, thus, plaintiffs could not establish standing); Complaint for Declaratory Judgment and Damages, Pascazi v. Verizon Commc'ns Inc., No. 06 Civ. 1221 (S.D.N.Y. Feb. 16, 2006); Complaint, Ctr. for Constitutional Studies v. Bush, No. 06-CV-00313 (S.D.N.Y. Jan 17, 2006).

stani group with scientific expertise may wish to export nuclear technologies to Muslim nations:

> If there's a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response . . . . It's not about our analysis, or finding a preponderance of evidence . . . . It's about our response.[563]

The prevention policy first announced by Attorney General Ashcroft shortly after September 11 is hardly the same as treating the one percent chance as certainty, but it is closer to policies that treat suspicion as probable cause. What are the marginal costs and benefits to our national security of laws and policies that base their operational terms on a "one percent chance," or even a reasonable suspicion of a horrific consequence? What values and legal safeguards are lost when traditional standards of proof and evidence are eschewed in favor of action based on suspicion or an indiscriminate data mining program? How does a program like TSP serve to disrupt or even expose al Qaeda or other would-be terrorists? And to what extent do secret surveillance initiatives like TSP corrode the democratic values and institutions that we seek to protect from terrorism? At a minimum, the unraveling of FISA and emergence of the TSP call into question the virtual disappearance of effective oversight of our national security surveillance. The Congress and federal courts have become observers of the system, not even participants, much less overseers.[564]

The circumstances that led to the enactment of FISA nearly thirty years ago—a chastened executive, an awakened Congress, courts newly willing to protect privacy in electronic surveillance settings—may never recur. The imperfect system for national security surveillance that FISA codified worked reasonably well through the early 1990's. As terrorism ascended in importance as a national security concern and Congress and the President worked to enact new laws criminaliz-

563. RON SUSKIND, THE ONE PERCENT SOLUTION: DEEP INSIDE AMERICA'S PURSUIT OF ITS ENEMIES SINCE 9/11, at 62 (2006) (quoting Vice President Richard Cheney); s*ee also id.* at 47–49 (discussing the background on the Pakistani group and its objectives).

564. Jack Balkin and Sanford Levinson argue that an emerging "National Surveillance State" will be driven principally by technological advances and national security interests. The executive branch will, they say, make decisions to displace the criminal justice system with security mechanisms and to make other elements of criminal justice like the national security system. Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 522–23 (2006).

ing terrorist activities, pressures on the FISA process increased and its careful accommodation of foreign intelligence and law enforcement interests was ensnared in bureaucratic confusion, institutional rivalries, and personal and inter-agency jealousies.[565]

When the Patriot Act followed soon after September 11, the institutional and bureaucratic barriers to sharing intelligence information that contributed to the failure to anticipate the hijackers were misapprehended and translated into a legal change to FISA that was showcased as breaking down the wall that kept us from preventing the attacks. The ensuing revision of Justice Department guidelines and their review by the FISC and FISCR struck a serious blow to the essential terms of the FISA arrangement—providing a mechanism for secret surveillance with reduced predicates for targeting, in return for a commitment that the special process would not be used by criminal prosecutors who simply could not meet the traditional warrant requirements. Now the fear expressed by the FISC in 2002—that abuses of FISA could increasingly occur—is not farfetched.

David Kris has pointed out an argument that keeping the wall down may enhance civil liberties. Kris reasons that, with the wall out of the way, "more DOJ lawyers may become involved in national security investigations. . . . More lawyers means more oversight, and lawyer oversight is how [we] protect[] civil liberties in intelligence." Second, Kris argued, using law enforcement to counter foreign threats is, considering alternative methods available to the government "among the most benign. The wall channels government toward more extreme measures."[566]

Kris correctly observes that the Church Committee Report concluded that tethering domestic security investigations to a legal framework under the supervision of the Attorney General was one of the fundamental correctives to the abuses uncovered.[567] As FISA, FBI Guidelines, and executive orders were

565. *See* WRIGHT, *supra* at note 191, 312–13 (maintaining that agency rivalries, institutional culture, and personal hatred between FBI and CIA officials contributed to failures to share intelligence).

566. David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 523–24 (2006).

567. *Id.* at 524; *see* 2 SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 332 (1976).

implemented, lawyers closely supervised the gathering of intelligence. According to Kris, the FISA wall kept lawyers in the field—those working with criminal investigators—away from intelligence investigations. After the FISCR decision, prosecutors in field offices of the Criminal Division and in U.S. Attorney's Offices have regular access to intelligence investigators. Their orientation toward preserving all criminal prosecution options makes them especially sensitive to rule violations that could affect the criminal case. Thus, Kris argues, "civil libertarians ought to oppose the wall and encourage increased prosecutorial involvement in national security investigations."[568]

Kris is, of course, speculating about the effects of the wall, pre- and post-FISCR. Based on its long experience with FISA, the 2002 en banc FISC was apparently more concerned with potential prosecutorial misuse of the FISA processes to *enhance* the prosecution option than it was with the absence of effective legal oversight of the implementation of FISA by intelligence professionals in the field. As noted earlier in this Article, the pre-certification involvement of legal review in assuring that FISA is properly applied in all respects, including that a significant purpose of the surveillance is to collect foreign intelligence, is extensive, far more so than the process that attends Title III warrant applications. I am inclined to respect the judgment of the experienced FISC judges on this important issue.

Kris's second claim, that after the fall of the wall, civil liberties are less threatened by the prosecution option more likely after the fall of the wall because of the "less gentle" options otherwise likely to be taken, is a reminder that our government has subjected even United States citizens to military detention since 2002. In other words, things could always be worse. To be sure, military detention is the greater threat to civil liberties than civilian prosecution. While the legal contours of permissible military detention and adjudication are not fully developed, it is highly unlikely that this draconian alternative to civilian prosecution would be undertaken on any kind of widespread basis.

The Justice Department has proudly showcased what it views as the tremendous benefits from the Patriot Act's information sharing provisions and the lowering of the wall. One

568. Kris, *supra* note 566, at 527.

example involved the Department's investigations of suspected al Qaeda cell members in Lackawanna, New York, the so-called "Lackawanna Six." The investigation began in the summer of 2001, based on an anonymous tip delivered to the FBI that local Yemeni-Americans might be involved in drug crime and terrorist activities. Initially, FBI "concluded that existing law required the creation of two separate investigations in order to retain the option of using FISA."[569] According to the Department, the Patriot Act made clear that information sharing between the two teams was allowed, which in turn let the criminal side know that an al Qaeda agent was involved, leading to early criminal charges against the six.[570] This Article has shown that neither the 1978 FISA nor the 2001 FISA, as amended by the Patriot Act, stood in the way of simultaneous investigations of the same target or targets, in parallel or as one team, so long as the purpose of the FISA investigation was the collection of foreign intelligence. The wall procedures that appeared in 1995 were not required by FISA and even those would have permitted the sharing that allegedly could not occur in the Lackawanna investigation, so long as the Criminal Division did not direct or control the FISA investigation.[571]

Meanwhile, rapid and accelerating changes in technology and in particular the digitization of surveillance and communications presented Congress and the President with ongoing challenges to keep up with and exceed the communications and evasion capabilities of adversaries. While FISA was amended toward these ends to the apparent satisfaction of the executive branch, the administration approved NSA surveillance and the TSP. Consistent with the prevention paradigm, the TSP eschews probable cause and individualized suspicion and judicial

569. U.S. DEP'T OF JUSTICE, REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK 3 (July 2004), *available at* http://www.fas.org/irp/agency/doj/patriot0704.pdf.

570. *Id.*

571. In addition to the Lackawanna investigation, the Justice Department lists seven other examples "made possible by the USA PATRIOT Act," *Id.* at 5. In all of them, the increased sharing of information and coordination between law enforcement and intelligence officers has resulted from changes in DOJ procedures and direction from senior officials, none of which was legally forbidden before the Patriot Act and the FISCR decision. The sharing and coordination contemplated by the 2002 Ashcroft guidelines would have been permitted without the Patriot Act changes. Indeed, the 2002 guidelines prescribe policies that sound quite similar to those practiced without the benefit of written rules during the OIPR tenure of Mary Lawton. *See supra* text accompanying notes 166–68.

and congressional oversight and review, all hallmarks of FISA. The extent to which digital capabilities render these central legal instruments obsolete is a complex topic that could only briefly be considered in this Article. Whatever the answer to this digital revolution, however, it is clear that what remains of FISA has been ignored.

In our legal system, we attach great importance to the value of fair processes. In national security law and policy, when secrecy has been an important operational requisite, we have developed review and oversight processes to help assure that unilateral power is not abused. So has it been with FISA. In the five years since September 11, those process safeguards have largely been lost or overtaken. If FISA is to have any meaningful role for the next thirty years, its central terms will have to be restored, one way or the other.