2005

The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law

Patricia E. Simone

Patricia L. Bellia
Notre Dame Law School, patricia.l.bellia.2@nd.edu

THE "LONE WOLF" AMENDMENT AND THE FUTURE OF FOREIGN INTELLIGENCE SURVEILLANCE LAW

PATRICIA L. BELLIA*

I. INTRODUCTION

ON August 16, 2001, agents of the Federal Bureau of Investigation (FBI) and the Immigration and Naturalization Service (INS) in Minneapolis detained French national Zacarias Moussaoui for a visa waiver violation.[1] Moussaoui came to the agents' attention after instructors at the Pan Am International Flight Academy in Eagan, Minnesota, found his behavior suspicious enough to report it to the Minneapolis field office of the FBI.[2] Moussaoui had sought training on Pan Am's Boeing 747 flight simulators, but lacked the ordinary qualifications for such training and disclaimed any interest in becoming a commercial pilot.[3] FBI agents soon learned that Moussaoui held jihadist beliefs and suspected that he was "an Islamic extremist preparing for some future act in furtherance of radical fundamentalist goals"—a future act that, the agents concluded, was somehow related to Moussaoui's flight training.[4]

To prevent Moussaoui from obtaining any further training, the FBI coordinated with the INS to have Moussaoui detained immediately.[5] Moussaoui declined to permit agents to search his belongings; after being informed that he would be deported, however, Moussaoui allowed the

* Lilly Endowment Associate Professor of Law, Notre Dame Law School. A.B. Harvard College, J.D. Yale Law School. I thank A.J. Bellia, Rick Garnett, Jimmy Gurulé, John Nagle, and participants at a faculty workshop at the University of Connecticut School of Law for helpful comments. This Article benefited from discussions with current and former federal officials with expertise in foreign intelligence surveillance law, many of whom would prefer not to be identified. Jeannette Cox and research librarian Patti Ogden provided outstanding research assistance.

1. *See* SENATE SELECT COMM. ON INTELLIGENCE & 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. 107-371, H.R. REP. NO. 107-792, at 318 (2002) (unclassified pagination), *available at* http://a257.g.akamaitech.net/7/257/2422/24jul20031400/www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf [hereinafter JOINT INQUIRY]. Because Moussaoui entered the United States on a French passport, he was permitted to remain for 90 days without a visa. He was out of legal immigration status after May 22, 2001. *See id.* at 316.

2. *Id.*

3. *See* NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 273 (Norton 2004) [hereinafter 9/11 COMMISSION REPORT]; JOINT INQUIRY, *supra* note 1, at 316.

4. 9/11 COMMISSION REPORT, *supra* note 3, at 273.

5. *Id.*; JOINT INQUIRY, *supra* note 1, at 317-18.

agents to take the items to the INS office for safekeeping.[6] Among Moussaoui's possessions was a laptop computer.[7] Over the next two weeks, Minneapolis FBI agents, in consultation with agents in the Radical Fundamentalist Unit at FBI Headquarters, worked to assemble sufficient information to request a court order under the Foreign Intelligence Surveillance Act (FISA)[8] authorizing a search of Moussaoui's computer and other possessions.[9] Believing the evidence to be insufficient to support a FISA request, attorneys at FBI Headquarters declined to proceed with the FISA process.[10] No order for a search of Moussaoui's belongings was obtained until after the September 11th terrorist attacks.

In the immediate aftermath of those attacks, it was widely believed that Moussaoui was the "missing" twentieth hijacker—the fifth member of the team assembled to hijack United Airlines Flight 93 out of Newark, which ultimately crashed in rural Pennsylvania.[11] The failure to fully investigate Moussaoui quickly became a focal point for criticism of law enforcement and intelligence efforts in the months leading up to the attacks. Indeed, the Final Report of the National Commission on Terrorist Attacks upon the United States characterized the government's stalled investigation of Moussaoui as a "missed opportunity."[12] A "maximum U.S. effort to investigate Moussaoui" and certain other dropped leads, the Report stated, could have "brought investigators to the core of the 9/11 plot" and possibly even derailed it.[13]

The Moussaoui episode eventually prompted a controversial legislative response. In December 2004, as part of a broad intelligence reform bill, Congress amended FISA to expand the government's power to conduct electronic surveillance and physical searches of suspected international terrorists.[14] FISA allows federal officials to obtain a court order

6. JOINT INQUIRY, *supra* note 1, at 318.

7. *Id.*

8. 50 U.S.C. §§ 1801-1863 (2000).

9. 9/11 COMMISSION REPORT, *supra* note 3, at 273-74; JOINT INQUIRY, *supra* note 1, at 319-20.

10. 9/11 COMMISSION REPORT, *supra* note 3, at 274; JOINT INQUIRY, *supra* note 1, at 321-22.

11. *See, e.g.*, Philip Shenon, *The 20th Suspect*, N.Y. TIMES, Oct. 16, 2001, at B5. More recent evidence apparently suggests that the fifth member of the United Airlines Flight 93 team was in fact intended to be Mohamed al Kahtani, who was refused entry into the United States on August 4, 2001. *See* 9/11 COMMISSION REPORT, *supra* note 3, at 11, 456 n.73. The 9/11 Commission Report identifies Moussaoui as a potential substitute pilot for United Airlines Flight 93. *See id.* at 246-47.

12. *See* 9/11 COMMISSION REPORT, *supra* note 3, at 273 ("If Moussaoui had been connected to al Qaeda, questions should instantly have arisen about a possible al Qaeda plot that involved piloting airliners, a possibility that had never been seriously analyzed by the intelligence community.").

13. *Id.* at 276.

14. *See* Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742. For the connection between the Moussauoi investigation and the legislation, see S. REP. NO. 108-40, at 3 (2003).

authorizing surveillance or a search to acquire "foreign intelligence information," including information relating to the United States' ability to protect itself against hostile acts, sabotage, international terrorism or clandestine intelligence activities.[15] A FISA order is available only if a judge of a special court, the Foreign Intelligence Surveillance Court (FISC), finds probable cause to believe that, among other things, the target of the surveillance or search is a "foreign power" or an "agent of a foreign power."[16]

As enacted in 1978, FISA defined the term "foreign power" to include "a group engaged in international terrorism or activities in preparation therefor,"[17] and defined the term "agent of a foreign power" to include both a member of such a group[18] and any person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, on behalf of a foreign power."[19] FISA has thus always been available as an investigative tool in some international terrorism cases. In the Moussaoui investigation, however, attorneys at FBI Headquarters believed that FISA's standards could not be met because the FBI had found no evidence that Moussaoui was a member of or affiliated with a terrorist group.[20] In other words, Moussaoui appeared to be a "lone wolf"—perhaps acting in sympathy with the aims of a terrorist group but not on its behalf, or perhaps acting on behalf of a terrorist group but in such a way that the requisite connection still could not be demonstrated.

The FISA amendment incorporated in the December 2004 intelligence reform bill sought to ensure that FISA coverage of lone wolf terrorists could more readily be obtained. Often referred to as the "Moussaoui fix" or "lone wolf amendment,"[21] the measure broadened the definition of an "agent of a foreign power" to include any non-U.S. per-

15. 50 U.S.C. § 1801(e)(1) (2000). The category of foreign intelligence information described in the text is often referred to as "protective" or "counterintelligence" information. *See* S. REP. NO. 95-701, at 9-10 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977; *In re* Sealed Case, 310 F.3d 717, 723 n.9 (Foreign Intel. Surv. Ct. Rev. 2002). FISA also covers the gathering of "positive" or "affirmative" foreign intelligence information. *See* 50 U.S.C. § 1801(e)(2); S. REP. NO. 95-701, at 9-10 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977; *In re* Sealed Case, 310 F.3d at 723 n.9 For further discussion of the scope of FISA, see *infra* notes 89-93 and accompanying text.

16. 50 U.S.C. § 1805(a)(3)(A).

17. *Id.* § 1801(a)(4).

18. *Id.* § 1801(b)(1)(A).

19. *Id.* § 1801(b)(2)(C).

20. As discussed below, there was some evidence linking Moussaoui to Chechen rebels. *See infra* notes 249-51 and accompanying text. Agents mistakenly believed that the Chechen rebels would not qualify as a terrorist group because they were not on the State Department's list of designated foreign terrorist investigations. *See* JOINT INQUIRY, *supra* note 1, at 321; 9/11 COMMISSION REPORT, *supra* note 3, at 274. Later evidence apparently revealed that Moussaoui was not working for the Chechen rebels. *See* S. REP. NO. 108-40, at 3 (2003).

21. *See* S. REP. NO. 108-40, at 2, 11 (2003).

son[22] who "engages in international terrorism or activities in preparation therefor."[23] As noted, FISA previously had required a showing that activities in which the target engaged were undertaken "for or on behalf of" a foreign power.[24] With respect to non-U.S. persons, then, the amendment essentially eliminates the requirement to link the target's activities to a foreign power or an agent of a foreign power.

At first, the logic of the lone wolf amendment seems quite compelling. Throughout hearings addressing law enforcement and intelligence issues in the post-9/11 world, government officials emphasized that the current terrorist threat is far different from anything Congress envisioned when FISA was passed in 1978. Many terrorist organizations lack a centralized, hierarchical structure; thus, individual terrorists can carry out activities in sympathy with a widespread anti-American movement, but not at the direction of any particular organization.[25] Moreover, because the lone wolf amendment is limited to non-U.S. persons.[26] and does not disturb the requirement to show that the target engages in activities in preparation for international terrorism,[27] the change, by initial appearances, has limited consequences for privacy. Finally, from a legislative process standpoint, the lone wolf amendment does not seem as vulnerable to criticism as the FISA changes adopted in the controversial Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act.[28] The Patriot Act was signed only seven weeks after the 9/11 attacks;[29] it took over two years for the lone wolf amendment to become law.[30]

---

22. Under FISA, a "United States person" covers U.S. citizens, permanent resident aliens, U.S. corporations and unincorporated associations substantially composed of U.S. citizens or permanent resident aliens. 50 U.S.C. § 1801(i).

23. *See* Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (to be codified at 50 U.S.C. § 1801(b)(1)(C)).

24. 50 U.S.C. § 1801(b)(2)(C).

25. *See, e.g., Amendments to the Foreign Intelligence Surveillance Act: Hearings on S. 2586 and S. 2659 Before the Senate Select Committee on Intelligence*, 107th Cong. 14-19, 20-21 (2003) (statement and testimony of Marion E. "Spike" Bowman, Deputy General Counsel, FBI).

26. *See* 50 U.S.C. § 1801(b)(1) (excluding U.S. persons); IRTPA § 6001(a), 118 Stat. at 3742 (adding new subsection to § 1801(b)(1)).

27. IRTPA § 6001(a), 118 Stat. at 3743.

28. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

29. I do not intend to endorse this criticism. For an insider's view of the legislative process that resulted in passage of the Patriot Act, see Beryl A. Howell, *Seven Weeks: The Making of the USA Patriot Act*, 72 GEO. WASH. L. REV. 1145 (2004).

30. The first version of the lone wolf amendment was introduced in the Senate on June 5, 2002, as S. 2586. *See* 148 CONG. REC. S5041 (daily ed. June 5, 2002) (introduced by Mr. Schumer). Despite the fact that the lone wolf amendment followed a separate track from the Patriot Act FISA amendments, the inclusion of a lone wolf provision in a January 2003 package of potential Justice Department proposals (derisively labeled "Patriot Act II") has led to a different set of process-based

The lone wolf amendment nevertheless offers a fascinating lens through which to examine foreign intelligence surveillance law, and highlights some of the critical questions facing Congress as the December 31, 2005, sunset date for many of the post-9/11 surveillance-related changes (including the lone wolf amendment itself) approaches.[31] As a substantive matter, the seemingly minor lone wolf change in fact goes to the heart of the constitutional issues that the foreign intelligence surveillance framework presents. Assessing how courts are likely to resolve constitutional challenges to the lone wolf amendment underscores the critical need for Congress to rethink not only FISA's scope and substantive standards, but also what I refer to as its "information structure"—the institutional mechanisms designed to generate the information necessary for evaluation of how the Executive and the FISC have implemented the foreign intelligence surveillance framework. As the foreign intelligence surveillance framework has evolved over the last 27 years, its information structure has largely been neglected.

A full exploration of the foreign intelligence surveillance framework and its information structure is a large project, and I undertake only a piece of that project here. Drawing upon the lone wolf example, I illustrate the challenges that Congress faces in balancing the government's need to obtain foreign intelligence information against privacy interests. Courts play a necessarily diminished role in this area—a fact that Congress recognized when it first enacted FISA, and for which it sought to compensate by providing mechanisms for congressional and (to a lesser extent) public evaluation of the FISA process. As the foreign intelligence surveillance framework has evolved, relatively little attention has been paid to such mechanisms. Indeed, in passing the lone wolf amendment in December 2004, Congress, for the first time, gave more systematic consideration to FISA's information structure.[32] The changes made, however, cannot bear the weight of the expanding foreign intelligence surveillance system.

This Article proceeds in three Parts. Part II introduces the political and constitutional backdrop for FISA's passage in 1978. It then examines the scope, substantive standards, and certain procedural features of FISA as enacted and highlights some of the significant changes to the foreign

concerns. *See* Domestic Security Enhancement Act of 2003, § 101, *at* http://www.publicintegrity.org/docs/PatriotAct/story_01_020703_doc_1.pdf (last visited Aug. 10, 2005).

31. Congress made the lone wolf amendment subject to the sunset date that applies to many of the surveillance-related changes in the Patriot Act, including all but one of the FISA changes. *See* IRTPA § 6001(b), 118 Stat. at 3742 (referencing sunset provision of "section 224 of Public Law 107-56 (115 Stat. 295)"); USA Patriot Act § 224, 115 Stat. at 295. The only FISA change not set to expire in 2005 is the change expanding the number of judges on the Foreign Intelligence Surveillance Court. *See* USA Patriot Act § 208, 115 Stat. at 283.

32. For further discussion of FISA's information structure, see *infra* notes 233-45 and accompanying text.

intelligence surveillance framework since then. Part III uses the lone wolf amendment to explore the broader constitutional issues surrounding the use of FISA. I argue that, purely as a predictive matter, courts evaluating whether to admit FISA-derived evidence are unlikely to invalidate a search authorized under the lone wolf amendment, just as they have historically been reluctant to question the FISA framework more generally. My point is not that the courts' approaches are wrong as a doctrinal or normative matter, but rather that these approaches have important implications for FISA's information structure, which I explore in Part IV.

II. THE FOREIGN INTELLIGENCE SURVEILLANCE FRAMEWORK

As enacted in 1978, FISA provided a mechanism for federal investigators to seek a special court order to conduct electronic surveillance in the United States to obtain foreign intelligence information.[33] The statute reflected both a recognition that such surveillance was essential to the national security of the United States and a concern that unfettered Executive discretion to engage in such surveillance was highly susceptible to abuse. Although FISA initially applied only to electronic surveillance, the statute now covers a far broader range of investigative activities. This Part provides an overview of the foreign intelligence surveillance framework by exploring FISA's background, enactment and evolution.

A. *The Political and Constitutional Context for FISA's Enactment*

To understand the current foreign intelligence surveillance framework, it is important to set the context for FISA's enactment in 1978.[34] Prior to FISA's passage, the executive branch had long engaged in warrantless electronic surveillance for national security purposes[35] and had argued that such surveillance was essential to the protection of the United States and the conduct of the nation's foreign affairs.[36] The Watergate era, however, brought to light extensive misuse of electronic surveillance.

33. The reference to surveillance "in the United States" is an oversimplification. FISA's geographic scope is determined by its definition of "electronic surveillance." *See* 50 U.S.C. § 1801(f) (2000). That definition generally encompasses surveillance activities where the United States is the locus of the surveillance device or all participants to the communication are in the United States, *see id.* § 1801(f)(2)-(4), but it also includes the acquisition of the contents of a wire or radio communication by intentionally targeting a known U.S. person in the United States, without regard to the location of the surveillance device, *see id.* § 1801(f)(1).

34. For helpful overviews of FISA's background, see William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1153-59 (2003); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1310-20 (2004).

35. *See* United States v. United States District Court for the E. Dist. of Mich. [hereinafter *Keith*], 407 U.S. 297, 310-11 (1972).

36. *See* S. REP. No. 95-694 pt. 1, at 9 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3910.

The scandal prompted Congress to form a special Senate committee, popularly known as the "Church Committee" after its chairman, Frank Church, to conduct a wide-ranging investigation of U.S. intelligence agencies.[37] The Committee's final report revealed that the government had invoked "national security" to justify extensive surveillance of Americans with no connection to foreign powers:

> Too many people have been spied upon by too many Government agencies and [too] much information has [been] collected. . . . The Government . . . has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity.[38]

Moreover, even with respect to surveillance practices that could, in theory, be justified by dangers presented by the targeted groups, the constitutionality of the Executive's surveillance activities was very much in doubt. Congress had never explicitly authorized or forbidden surveillance for national security purposes. The 1968 statute authorizing and constraining the use of electronic surveillance in connection with criminal investigations, Title III of the Omnibus Crime Control and Safe Streets Act ("Title III"),[39] contained a proviso stating that nothing in the statute "shall limit the constitutional power of the President" to take certain measures deemed necessary to protect the United States.[40] Although the executive branch argued that this provision confirmed a presidential power to engage in warrantless electronic surveillance for national security purposes, the Supreme Court interpreted the language to leave any power that might exist undisturbed.[41] From a separation of powers perspective, then, the unanswered question at the time of FISA's passage was whether the "executive Power" lodged in the President by the Constitution[42] encompassed a power to engage in surveillance activities without any statutory authorization.

In addition, warrantless electronic surveillance raised obvious Fourth Amendment questions that had never been squarely addressed by the Supreme Court. The Court had ruled in the 1928 case of *Olmstead v. United*

37. *See* SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, BOOK II (1976).

38. *Id.* at 5.

39. Pub. L. No. 90-351, tit. III, §§ 801-804, 82 Stat. 200, 211-23 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2002)).

40. *See id.* § 802, 82 Stat. at 214 (adding § 2511(3)).

41. *See Keith*, 407 U.S. 297, 303 (1972).

42. U.S. CONST. art. II, § 1.

States[43] that a wiretap effected without a trespass onto private property did not violate the Fourth Amendment.[44] For nearly four decades, the constitutionality of electronic surveillance turned on whether placement of a particular surveillance device involved trespassory conduct—an approach that produced seemingly arbitrary results.[45] In the 1967 case of *Katz v. United States*,[46] the Court abandoned the trespass approach and held that the Fourth Amendment does not simply protect against government intrusions into physical areas in which an individual has a property interest: "[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[47]

Although *Katz* made clear that any violation of the privacy upon which a surveillance target "justifiably relied"[48]—a formula that soon evolved into the current "reasonable expectation of privacy" test[49]—would ordinarily require a warrant, the Court explicitly reserved the question of how its analysis would apply to "national security" surveillance.[50] In a footnote, the Court observed that "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[51] The issue was, however, a subject of debate among the concurring Justices. Justice White argued that "[w]e should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[52] Justice Douglas, joined by Justice Brennan, replied that Justice White sought to grant "a wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in

43. 277 U.S. 439 (1928).

44. *See id.* at 466.

45. *See, e.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1389 n.71 (2004); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 22 & n.71 (2004).

46. 389 U.S. 347 (1967).

47. *Id.* at 353.

48. *Id.*

49. The Court did not explain the circumstances in which one might "justifiably rel[y]" on privacy, but Justice Harlan's concurrence described the appropriate inquiry as encompassing two questions: whether "a person [has] exhibited an actual (subjective) expectation of privacy," and whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring). The Court adopted this formulation in subsequent cases. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979).

50. *Katz*, 389 U.S. at 358 n.23.

51. *Id.*

52. *Id.* at 364 (White, J., concurring).

cases which the Executive Branch itself labels 'national security' matters."[53]

In debating the applicability of the warrant requirement to surveillance for national security purposes in *Katz*, none of the Justices specified precisely what was meant by "national security." The Presidential measures that Congress carved out of Title III included not only measures deemed necessary to protect against hostile acts of a "foreign power," but also measures deemed necessary to protect against "the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government"[54]—dangers that could presumably come from purely domestic as well as foreign groups.

The Supreme Court addressed the constitutionality of the use of warrantless electronic surveillance against a purely *domestic* group in *United States v. United States District Court of the Eastern District of Michigan*, commonly known as the *Keith* case (for the name of the district court judge against whom the Government sought a writ of mandamus, Damon J. Keith of the Eastern District of Michigan).[55] The underlying dispute involved a criminal prosecution of individuals alleged to have conspired in the bombing of a CIA office in Michigan.[56] During pretrial proceedings, the defendants sought disclosure of information obtained through electronic surveillance and requested a hearing to determine whether this information, which the defendants claimed was obtained in violation of the Fourth Amendment, tainted other evidence the Government intended to offer.[57]

The Government acknowledged that its agents had indeed conducted warrantless surveillance against one of the defendants. The Government claimed, however, that the surveillance was lawful because it was undertaken under the President's power to safeguard national security.[58] The Government conceded that any threat to national security was purely internal: An affidavit of the Attorney General submitted in connection with the case stated that the surveillance had been "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of the Government."[59] Judge Keith concluded that the warrantless surveillance violated the Fourth Amendment and ordered disclosure of the surveillance tapes, and the Court of Appeals for the Sixth

53. *Id.* at 359 (Douglas, J., concurring).

54. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 200, 214 (adding § 2511(3)).

55. *Keith*, 407 U.S. 297 (1972).

56. *Id.* at 299.

57. *Id.* at 299-300.

58. *Id.* at 300-01.

59. *Id.* at 300 n.2 (emphasis added); *see also id.* at 308-09 (emphasizing that case involved no evidence of involvement of foreign power).

Circuit denied the Government's petition for a writ of mandamus to set aside the order.[60]

The Supreme Court agreed with the lower courts that the surveillance violated the Fourth Amendment.[61] Because the case involved a purely domestic group, the Court framed the inquiry as whether there was something special about domestic surveillance security cases to necessitate an exception to the Fourth Amendment's warrant requirement.[62] The Government argued that, in two ways, applying the warrant requirement would unduly frustrate the government's efforts to protect itself from acts of subversion and overthrow. First, in light of the "complex and subtle factors" involved in national security matters, courts would lack the expertise to determine whether "'there was probable cause to believe that surveillance was necessary to protect national security.'"[63] Second, the disclosure of information that would necessarily accompany the submission of a warrant application to a judge would risk compromising the secrecy essential to intelligence gathering.[64] The *Keith* Court rejected each of these arguments, stating that the Government's concerns "do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval."[65]

Although the *Keith* Court faced only a narrow question concerning the constitutionality of warrantless surveillance in cases involving purely domestic threats to national security, the Court made broader observations that influenced Congress's approach in FISA. First, in confining its holding to cases involving security threats from *domestic* groups, the Court implied that the Executive would be freer to act and Congress would be freer to legislate with respect to security threats that were not purely domestic—threats that the Court identified as involving "foreign powers" or their "agents."[66] In a footnote, the Court elaborated as follows on its distinction between threats from purely domestic organizations and threats from groups with a connection to a foreign power: "[W]e use the term 'domestic organization' in this context to mean a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a *foreign power, its agents or agencies.*"[67]

60. United States v. United States District Court for the E. Dist. of Mich., 444 F.2d 651, 667 (6th Cir. 1971).

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

62. *Id.* at 318.

63. *Id.* at 319.

64. *Id.*

65. *Id.* at 321.

66. *See id.* at 308 (observing that case required "no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers"); *id.* at 309 (noting absence of evidence of "any involvement, directly or indirectly, of a foreign power"); *id.* at 322 (emphasizing that Court expressed no view on issues involved "with respect to activities of foreign powers or their agents").

67. *Id.* at 309 n.8 (emphasis added).

Second, the Court raised the possibility that the same standards and procedures that apply in criminal cases may not necessarily be appropriate or required in national security cases, even those involving purely domestic threats:

> We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crimes specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.[68]

Accordingly, standards differing from those governing electronic surveillance in criminal cases "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[69] The Court further opined that Congress might judge that "the application and affidavit showing probable cause need not follow" the exact standards of Title III, but should "allege other circumstances more appropriate to domestic security cases."[70] The Court also suggested that a request for court authorization for national security surveillance could be made to a specially designated court.[71]

Because the *Keith* decision did not foreclose warrantless surveillance in cases involving foreign powers or their agents, the Executive continued to conduct warrantless surveillance to gather foreign intelligence information.[72] In challenges to the use, in criminal cases, of evidence derived from such surveillance, three courts of appeals concluded that wiretaps conducted for the purpose of gathering foreign intelligence information were lawful despite the absence of a warrant.[73] A plurality of the Court of

68. *Id.* at 322.

69. *Id.* at 322-23.

70. *Id.* at 323.

71. *Id.*

72. *Id.*

73. *See* United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement . . . ."); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (deeming surveillance lawful when district court had found that such surveillance was "conducted and maintained solely for the purpose of gathering foreign intelligence information"); United States v. Brown, 484 F.2d 418, 425 (5th Cir. 1973) (finding warrantless wiretaps conducted "for the purpose of obtaining foreign intelligence" lawful).

Appeals for the D.C. Circuit, however, addressing an issue not squarely presented in the case before it, questioned whether there could be any "foreign intelligence" exception to the warrant requirement.[74]

In the wake of *Keith* and its progeny, then, the Fourth Amendment issues raised by foreign intelligence surveillance had not been fully resolved. Against this constitutional backdrop, and in a political climate of deep suspicion of government surveillance in the name of national security, FISA reflected a compromise: Congress authorized but constrained the use of electronic surveillance techniques to gather foreign intelligence information. By providing explicit statutory authorization, Congress eliminated the separation of powers question—whether the executive power lodged in the President encompassed the power to engage in surveillance activities without any statutory authorization. At the same time, Congress did not leave the determination of when surveillance was appropriate wholly to the Executive's discretion: Congress required the Executive to present a surveillance application to a judicial authority. Congress thus blunted some—although certainly not all—Fourth Amendment concerns that the previous era of unchecked electronic surveillance had raised. Legislating in the shadow of the *Keith* case, Congress tied the availability of surveillance under FISA to the Government's ability to show that the target was a "foreign power" or an "agent of a foreign power," and set forth procedures differing from those in Title III. The next section explores the statute in further detail.

B. *Foreign Intelligence Surveillance Law in 1978*

As passed in 1978, FISA contained a single substantive title governing electronic surveillance activities in the United States.[75] The statute was subsequently amended to govern physical searches,[76] acquisition of communications attributes,[77] and compelled production of certain records

74. *See* Zweibon v. Mitchell, 516 F.2d 594, 613 (D.C. Cir. 1975) (en banc) (plurality opinion) (analyzing whether foreign intelligence warrant requirement exists). Because *Zweibon* involved warrantless surveillance "in the name of foreign intelligence gathering for protection of the national security," but directed at a purely domestic group not alleged to be "the agent of [or] acting in collaboration with a foreign power," the court did not need to address whether the Fourth Amendment permitted surveillance directed at a foreign power or its agents. *Id.* at 614. The plurality nevertheless stated that "an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional." *Id.* at 613-14.

75. *See* Foreign Intelligence Surveillance Act (FISA), Pub. L. No. 95-511, 92 Stat. 1783, 1783 (1978). Two additional titles set forth conforming amendments and the statute's effective date.

76. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified as amended at 50 U.S.C. §§ 1821-1829 (2000 & Supp. I 2001)).

77. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2405 (codified as amended at 50 U.S.C. §§ 1841-46 (2000 & Supp. I 2001)). The term "communications attributes" is Susan

and tangible things.[78] In addition, Congress enacted other statutes providing related investigative authorities and tied their standards to FISA.[79] To facilitate discussion of the foreign intelligence surveillance framework as a whole, as well as a comparison to criminal search authorities, I focus on three aspects of FISA as enacted: (1) the *scope* of orders authorized under the statute; (2) the *standard* that the government must meet to trigger FISA coverage; and (3) the related *procedural features* of the statutory scheme.

A brief discussion of judicial involvement in the FISA process is in order. As noted, in the *Keith* case the Supreme Court had raised the possibility that requests for domestic security surveillance could be made to a specially designated court, offering the federal district and appeals courts in the District of Columbia as examples. FISA took up the Court's invitation to route requests for surveillance involving national security to a specific forum and created a special federal court for that purpose. FISA requires the Chief Justice of the United States to designate a number of federal judges—initially seven; increased to eleven by the USA Patriot Act—to "constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance."[80] The judges serve non-renewable seven-year terms.[81] The FISC judges sit individually[82] on a rotating basis, holding classified, *ex parte* proceedings in a secure facility in the Justice Department.[83] Attorneys from the Depart-

---

Freiwald's. *See* Freiwald, *supra* note 45, at 46; Susan Freiwald, *Uncertain Privacy: Communications Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 951-60 (1996).

78. *See* Intelligence Authorization Act for Fiscal Year 1999, § 602, 112 Stat. at 2410 (codified at 50 U.S.C. § 1862 (2000)) (authorizing orders to compel production of certain business records); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified at 50 U.S.C. §§ 1861-1862 (Supp. I 2001)) (deleting former §§ 1861-1863 and adding new §§ 1861-1862 authorizing orders to compel production of tangible things).

79. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (codified as amended at 18 U.S.C. § 2709 (2000 & Supp. I 2001)); Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99-569, § 404, 100 Stat. 3190, 3197 (1986) (codified as amended at 12 U.S.C. § 3414(a)(5)(A) (Supp. I 2001)); Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601, 109 Stat. 961, 974 (codified as amended at 15 U.S.C. § 1681u(a)-(c)) (Supp. I 2001)).

80. 50 U.S.C. § 1803(a) (2000 & Supp. I 2001); *see* FISA § 103(a), 92 Stat. at 1788; USA Patriot Act § 208, 115 Stat. at 283.

81. 50 U.S.C. § 1803(d).

82. The full court has conducted one proceeding involving all of its members, which it labeled as an "en banc" proceeding. *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002). For further discussion of this case, see *infra* notes 190-91 and accompanying text.

83. *See* Benjamin Wittes, *Inside America's Most Secretive Court*, LEGAL TIMES, Feb. 19, 1996, at 1. The use of the Justice Department's secure facilities is not specified in the statute; FISA requires that proceedings be conducted "as expeditiously as

ment's Office of Intelligence Policy and Review appear before the court to present applications for FISA coverage on behalf of the executive branch.[84] FISA also requires the Chief Justice to designate three federal judges to serve as a court of review in connection with the denial of FISA applications.[85]

1. *Scope*

As passed, FISA governed only "electronic surveillance" to obtain "foreign intelligence information."[86] The term "electronic surveillance" has an extremely complex definition, but essentially regulates acquisition of the contents of communications through the monitoring of persons or the installation of surveillance devices within the United States.[87] The term "foreign intelligence information" is defined to cover two broad categories of information. Section 1801(e)(2) of FISA includes information that might be described as "positive" (or "affirmative") foreign intelligence information[88]—information with respect to a foreign power or foreign territory that relates to "the national defense or the security of the United States" or "the conduct of the foreign affairs of the United States."[89]

Section 1801(e)(1) covers information that might be described as "counterintelligence" (or "protective") information[90]—information relating to the United States' ability to protect against "grave hostile acts of a foreign power or an agent of a foreign power,"[91] "sabotage or international terrorism by a foreign power or an agent of a foreign power,"[92] or "clandestine intelligence activities"[93] by a foreign power or an agent of a foreign power. Although the foreign intelligence information definition is important to FISA's scope, FISA's substantive standards do not require a showing that an investigation will in fact yield foreign intelligence information. Rather, as discussed below, the substantive standards focus on the officials' intent to acquire such information.

---

possible" and that "[t]he record of proceedings under this chapter, including applications made and orders granted, shall be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence." 50 U.S.C.A. § 1803(c) (West 2005).

84. *See* Wittes, *supra* note 83, at 1.

85. *See* 50 U.S.C. § 1803(b) (2000).

86. *See* 50 U.S.C. §§ 1803(a), 1804(a)(7)(A)-(B).

87. *See id.* § 1801(f). For further discussion of § 1801(f), see *supra* note 33 and accompanying text.

88. *See* S. REP. No. 95-701, at 9-10 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3977-78; *see also In re* Sealed Case, 310 F.3d 717, 723 n.9 (Foreign Intel. Surv. Ct. Rev. 2002).

89. 50 U.S.C. § 1801(e)(2).

90. *See* S. REP. No. 95-701, at 9-10, *reprinted in* 1978 U.S.C.C.A.N. 3973 at 3978; *see also In re* Sealed Case, 310 F.3d at 723 n.9.

91. 50 U.S.C. § 1801(e)(1)(A).

92. *Id.* § 1801(e)(1)(B).

93. *Id.* § 1801(e)(1)(C).

2. *Substantive Standards*

FISA requires that an application for an order approving electronic surveillance be made by a federal officer "in writing upon oath or affirmation" to a judge of the FISC.[94] Before the submission of the application to the FISC, the Attorney General or Deputy Attorney General[95] must find that the application meets FISA's requirements. Although those requirements are numerous, two are especially important.

FISA first requires a showing that the surveillance will yield communications of a "foreign power" or an "agent of a foreign power." In particular, an application must provide a statement of the facts and circumstances showing that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[96] A FISC judge can approve the surveillance only if he or she finds probable cause to believe that the application's assessments concerning the target and the facilities are correct. The "foreign power" and "agent of a foreign power" definitions are thus critical to the statute's scope, but their coverage is quite complicated.

The term "foreign power" includes not only so-called "official"[97] foreign powers (such as foreign governments, factions of foreign nations and entities acknowledged to be controlled by foreign governments),[98] but also "unofficial" foreign powers, including groups engaged in international terrorism.[99] The statute's "agent of a foreign power" definition differs according to whether or not the target is a U.S. person. Under FISA as enacted in 1978, any person "other than a United States person" could be treated as an agent of a foreign power if he or she acted (A) as an officer or employee of a foreign power or a member of an international terrorist group;[100] or (B) on behalf of a foreign power that engages in clandestine intelligence activities in the United States, when "the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States."[101]

---

94. *Id.* § 1804.

95. FISA uses the term "Attorney General," but defines it to include "the Attorney General of the United States (or Acting Attorney General) or the Deputy Attorney General." *Id.* § 1801(g).

96. *Id.* § 1804(a)(4).

97. *See* S. REP. No. 95-701, at 16-17 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3985-86.

98. *See* 50 U.S.C. § 1801(a)(1)-(3).

99. *See id.* § 1801(a)(4). Other unofficial foreign powers include "a foreign-based political organization, not substantially composed of United States persons," or "an entity that is directed and controlled by a foreign government or governments." *Id.* § 1801(a)(5)-(6).

100. *Id.* § 1801(b)(1)(A).

101. *Id.* § 1801(b)(1)(B).

Any person, including a U.S. person, could be treated as an agent of a foreign power if he or she (A) knowingly engaged in clandestine intelligence gathering activities on behalf of a foreign power, "which activities involve or may involve a violation of the criminal statutes of the United States;"[102] (B) knowingly engaged in any other clandestine intelligence activities on behalf of a foreign power, "which activities involve or are about to involve a violation of the criminal statutes of the United States;"[103] (C) knowingly engaged in "sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;"[104] or (D) aided or abetted any person or conspired with any person to engage in the prohibited activities.[105]

The second critical requirement concerns the purpose of the surveillance. As noted, FISA governs acquisition of "foreign intelligence information." To ensure that FISA is being properly used to obtain such information, the statute requires that a FISA application contain a series of certifications by any one among a group of designated executive branch officials, appointed by the President with the advice and consent of the Senate, "employed in the area of national security or defense."[106] The official must certify that he or she "deems the information sought to be foreign intelligence information."[107]

In addition, as enacted in 1978, FISA required that the official certify that "*the purpose* of the surveillance is to obtain foreign intelligence information."[108] (I discuss below the significance of the USA Patriot Act's change to that language.[109]) Because the Attorney General must determine that the application satisfies FISA before it is submitted, he or she implicitly certifies what the national security official certifies explicitly. If the target of the surveillance is a U.S. person, the FISC judge reviews the certifications for clear error.[110] If the target is not a U.S. person, the FISC

---

102. *Id.* § 1801 (b)(2)(A).

103. *Id.* § 1801(b)(2)(B). The activities also must be undertaken "pursuant to the direction of an intelligence service or network of a foreign power." *Id.*

104. *Id.* § 1801(b)(2)(C).

105. *See id.* § 1801(b)(2)(E). This provision was initially codified at § 1801(b)(2)(D). In 1999, Congress added a new § 1801(b)(2)(D), defining "agent of a foreign power" to include one who "knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power, or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power." *See* Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, § 601, 113 Stat. 1606, 1619 (1999).

106. 50 U.S.C. § 1804(a)(7). The currently designated officials include the Secretary and Deputy Secretary of State, the Secretary and Deputy Secretary of Defense, the Director and Deputy Director of Central Intelligence and the Director of the Federal Bureau of Investigation. *See* Exec. Order No. 12,139, 44 Fed. Reg. 30,311 (May 23, 1979).

107. 50 U.S.C. § 1804(a)(7)(A).

108. *Id.* § 1804(a)(7)(B) (emphasis added).

109. *See infra* notes 178-98 and accompanying text.

110. 50 U.S.C. § 1805(a)(5).

judge simply ensures that the application includes the proper statements and certifications.[111]

FISA coverage is thus available only if a judge of the FISC finds probable cause to believe that a target is a foreign power or an agent of a foreign power, and that a national security official has appropriately certified the purpose of the surveillance. Of particular interest is how these substantive standards relate to those that would apply to electronic surveillance in a criminal investigation—i.e., those set forth in Title III.

Title III requires an applicant to make a showing that, and a judge to find probable cause to believe that, a particular criminal offense is being committed and that targeting a specified facility will yield communications concerning the offense.[112] Although FISA similarly requires a finding of "probable cause," it does not explicitly require probable cause to believe that a crime has been, is being, or is about to be committed, or that targeting the specified facilities will yield communications relating to a crime. Rather, it requires probable cause to believe that the surveillance target is a "foreign power" or an "agent of a foreign power," and that the facilities are about to be used by such a power or agent.

Despite the absence of a requirement that a judge find probable cause of criminal activity, there is a substantial overlap between activities that make a target a foreign power or an agent of a foreign power and those that constitute criminal activity. For example, FISA coverage can be triggered by clandestine intelligence activities and international terrorism on behalf of a foreign power, both of which would typically involve criminal conduct.[113] The overlap, however, is not complete. Status as a "foreign power" is sufficient to trigger FISA coverage,[114] but does not necessarily imply criminal activity.[115] In addition, the first non-U.S. person definition of "agent of a foreign power" appears to apply a purely non-criminal standard: the alien's status as an officer or employee of a foreign power, rather than any particular activities, triggers FISA's coverage.[116] Other definitions permit FISA coverage when conduct "may" involve crim-

111. *Id.*

112. For further discussion of these Title III requirements, see Bellia, *supra* note 45, at 1390.

113. *See* 50 U.S.C. § 1801(b)(2). FISA defines international terrorism to include acts "that would be a criminal violation if committed within the jurisdiction of the United States or any State." *Id.* § 1801(c). It thus technically permits FISA coverage even for conduct that could not be prosecuted by the United States. *Id.* § 1801(c)(1).

114. *See id.* § 1804(a)(4)(a).

115. *Id.* § 1804.

116. *See id.* § 1801(b)(1)(A); S. REP. NO. 95-701, at 19 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3988.

inal activity[117]—a lower standard than the Fourth Amendment typically requires for a warrant.[118]

3. *Procedural Provisions*

FISA's procedural provisions also differ somewhat from those that apply to surveillance orders under Title III. A judge granting a Title III order can authorize surveillance for a period of up to thirty days; a court may grant extensions for up to thirty days, but only upon the same showings and findings as the original order.[119] The duration of a FISA electronic surveillance order depends on the type of target involved. As enacted in 1978, FISA allowed surveillance of an "official" foreign power for up to one year[120] and surveillance of other targets for ninety days.[121] A FISA order can be renewed upon an application to the FISC that meets the standards governing initial orders.[122] As passed, FISA allowed renewals "on the same basis as an original order," except that surveillance of certain unofficial foreign powers could proceed for up to one year if the judge found "probable cause to believe that no communication of any individual United States person will be acquired during the period."[123]

A second important procedural difference between the statutes concerns the issue of notice. Title III generally requires notice to the target (and, subject to the judge's discretion, other parties to intercepted communications) "[w]ithin a reasonable time but not later than ninety days" after termination of the surveillance.[124] The notice may be postponed upon a showing of good cause.[125] Under FISA, notice is not required as a matter of routine. Notice is required only when a government entity intends to introduce information obtained or derived from electronic surveillance in a judicial or other proceeding.[126]

117. *See, e.g.*, 50 U.S.C. § 1801(b)(1)(B) (permitting FISA coverage based on indication that target "may engage" in clandestine intelligence activities contrary to interests of United States); *id.* § 1801(b)(2)(A) (permitting FISA coverage of activities that "involve or *may involve*" violation of federal law) (emphasis added).

118. *See In re* Sealed Case, 310 F.3d 717, 738 (Foreign Intel. Surv. Ct. Rev. 2002) (noting that "Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases"). For discussions of the reach of the provision, see H.R. REP. NO. 95-1283, at 39-40 (1978) (noting that "may involve" standard covers "the situation where the Government cannot establish probable cause that the foreign agent's activities involve a specific criminal act, but where there are sufficient specific and articulable facts to indicate that a crime may be involved").

119. *See* 18 U.S.C. § 2518(5) (2000).

120. *See* 50 U.S.C. § 1805(e)(1).

121. *Id.*

122. *Id.* § 1805(e)(2).

123. *Id.*

124. 18 U.S.C. § 2518(8)(d).

125. *Id.*

126. *See* 50 U.S.C. § 1806(c)-(d). FISA also generally requires notice when the Attorney General approves electronic surveillance on an emergency basis and a request for a court order is subsequently denied. *See id.* § 1806(j).

C. *FISA's Evolution*

As passed in 1978, FISA applied only to electronic surveillance. FISA's scope, substantive standards and procedural provisions, however, have evolved significantly since the statute's enactment.

1. *Physical Searches*

The first major amendment to FISA occurred in 1994.[127] Despite the fact that FISA by its terms only governed electronic surveillance, the Carter Administration adopted a practice of seeking the FISA court's approval for physical searches to gather foreign intelligence information, on the theory that it was appropriate as a policy matter to have uniform treatment of different categories of foreign intelligence searches.[128] Officials in the Reagan Administration took a different view: that submitting physical search requests for judicial approval encroached upon the Executive's inherent authority to conduct warrantless searches for foreign intelligence purposes.[129]

In 1981, the Justice Department submitted a request for an order authorizing a physical search to the FISC and urged its denial.[130] When the FISC denied the order,[131] the Executive resumed a practice of conducting warrantless physical searches.[132] This practice continued through subsequent administrations. One such search was conducted during the 1993 investigation of suspected spy Aldrich Ames.[133] Concern arose within the Justice Department that, in a criminal prosecution, a district court would deem the warrantless search unconstitutional.[134] Although Ames's guilty plea eliminated this issue, the Executive sought an amendment to FISA governing physical searches, and Congress added physical search authority to FISA in 1994.[135]

---

127. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified as amended at 50 U.S.C. §§ 1821-1829 (2000 & Supp. I 2001)).

128. *See* H.R. REP. NO. 96-1466, at 5, 8-24 (1980).

129. *See* S. REP. NO. 97-280, at 4 (1981).

130. *Id.* (noting that Justice Department submitted application with memorandum of law contending that FISC lacked jurisdiction to approve physical searches).

131. *See* In the Matter of the Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Pers. Prop. (Foreign Intel. Surv. Ct. June 11, 1981), *reprinted in* S. REP. NO. 97-280, at 16-19 (1981).

132. *See* Exec. Order No. 12,333, § 2.5, 46 Fed. Reg. 59,941 (Dec. 8, 1981) (delegating to Attorney General power to approve use of techniques "for which a warrant would be required if undertaken for law enforcement purposes"); *see also* S. REP. NO. 98-660, at 17 (1984) (noting that Attorney General had approved physical searches "sparingly").

133. *See* S. REP. NO. 103-296, at 40 (1994).

134. *Id.*

135. *Id.*

The substantive standards for physical searches largely tracked those for electronic surveillance, requiring a showing of probable cause to believe that the target of the search is a foreign power or an agent of a foreign power,[136] and that "the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power."[137] In terms of procedural provisions, the statute permitted approval of a physical search "for the period necessary to achieve its purpose, or for forty-five days, whichever is less."[138] For searches of official foreign powers, the approval could last for up to one year.[139] As with electronic surveillance, the physical search provisions allowed renewals "on the same basis as an original order," except that surveillance of certain unofficial foreign powers could proceed for up to one year if the judge found "probable cause to believe that no property of any individual United States person will be acquired during the period."[140]

2. *Communications Attributes and Business Records*

The next significant amendment to FISA occurred in 1998, when Congress granted the FISC jurisdiction to grant orders authorizing use of "pen registers" and "trap-and-trace devices"[141]—that is, devices designed to detect communications attributes, such as the origin or destination of a wire or electronic communication—and orders compelling production of certain business records, namely those of a common carrier, vehicle rental facility, physical storage facility or public accommodation facility.[142] The substantive standard for the FISC's evaluation of such applications differed significantly from that governing electronic surveillance or physical searches.

For pen registers and trap-and-trace devices, rather than requiring probable cause to believe that the target was a foreign power or agent of a foreign power, the statute required a certification that use of the device would yield information that was "relevant" to an ongoing foreign intelligence or international terrorism investigation.[143] That standard roughly

136. 50 U.S.C. § 1824(a)(3)(A) (2000).

137. *Id.* § 1824(a)(3)(B).

138. *Id.* § 1824(d)(1).

139. *Id.*

140. *Id.* § 1824(d)(2).

141. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2405 (codified as amended at 50 U.S.C. §§ 1841-1846 (2000 & Supp. I 2001)).

142. *See* Intelligence Authorization Act for Fiscal Year 1999, § 602, 112 Stat. at 2410 (codified at 50 U.S.C. § 1862 (2000)) (authorizing orders to compel production of certain business records); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified at 50 U.S.C. §§ 1861-1862 (Supp. I 2001)) (deleting former §§ 1861-1863 and adding new §§ 1861-1862 authorizing orders to compel production of tangible things).

143. 50 U.S.C. § 1842(c)(2).

tracked that of the analogous criminal law authority, which required a certification of relevance to an ongoing criminal investigation.[144] The FISA pen/trap authority also had a second requirement: to demonstrate "reason to believe" that the target communications facility had been or would be used in connection with a suspected international terrorist, spy, foreign power or agent of a foreign power.[145] The substantive showing required for an order compelling production of business records order was similar to that for pen register and trap-and-trace devices: "relevance" to a foreign intelligence or international terrorism investigation, and specific and articulable facts giving reason to believe that the records concerned a foreign power or an agent of a foreign power.[146]

3. *National Security Letters*

An analysis of the scope and substantive standards of the foreign intelligence surveillance framework would be incomplete without consideration of three statutes not codified as part of FISA, but directly related to it. The statutes, including two passed in 1986 and one passed in 1996, grant FBI investigators the authority in certain foreign intelligence investigations to issue so-called "national security letters" (NSLs) compelling a third party to produce certain kinds of records. Such requests are not presented to the FISC or any other court, and in that sense the statutes are analogous to those granting agencies administrative subpoena authority. The records covered include transactional records from providers of wire and electronic communication services;[147] financial records from financial institutions;[148] and information concerning financial institutions and identifying information from credit reporting agencies.[149]

As passed, each statute permitted the FBI to issue NSLs upon written certification of two circumstances: that the records sought were connected to a foreign intelligence investigation,[150] and that there were specific and articulable facts linking the information sought to a foreign power or

144. 18 U.S.C. § 3123(a)(1) (2000).

145. *See* 50 U.S.C. § 1842(c)(3).

146. *Id.* § 1861(b)(2).

147. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (codified as amended at 18 U.S.C. § 2709 (2000 & Supp. I 2001)).

148. *See* Intelligence Authorization Act for Fiscal Year 1987, Pub. L. No. 99-569, § 404, 100 Stat. 3190, 3197 (1986) (codified as amended at 12 U.S.C. § 3414(a)(5)(A) (Supp. I 2001)).

149. *See* Intelligence Authorization Act for Fiscal Year 1996, Pub. L. No. 104-93, § 601, 109 Stat. 961, 974 (codified as amended at 15 U.S.C. § 1681u(a)-(c) (Supp. I 2001)).

150. More specifically, the provision concerning transactional records held by a wire or electronic communications provider required certification that the records were relevant to an "authorized foreign intelligence investigation," 18 U.S.C. § 2709 (2000); the financial records provision required certification that the records were "sought for foreign counterintelligence purposes," 12 U.S.C. § 3414(a)(5)(A) (2000); and the credit reporting provision required certification

agent of a foreign power under FISA.[151] In other words, although the NSL authorities were not part of FISA and did not involve the FISC, use of the provisions depended upon a showing of a link to a foreign power or agent of a foreign power under FISA.[152]

Prior to passage of the USA Patriot Act in 2001, then, the foreign intelligence surveillance framework could be summarized as follows. FISA contained two titles, one permitting requests for orders authorizing electronic surveillance and the other permitting requests for orders authorizing physical searches. Both sets of provisions required the applicant to demonstrate probable cause to believe that the target of the surveillance or search was a foreign power or an agent of a foreign power, and required a national security official to certify that "the purpose" of the surveillance was to gather foreign intelligence information. FISA also contained two other titles, one permitting requests for orders to acquire communications attributes and the other permitting orders to compel production of certain business records. Both sets of provisions required a showing of relevance to a foreign intelligence investigation, as well as a strong link between the information sought and a foreign power or agent of a foreign power. Finally, three other authorities permitted the FBI to compel production of certain records without a court order, but upon certification that the information sought was connected to a foreign intelligence investigation and that there were specific and articulable facts linking the records to a foreign power or an agent of a foreign power.

4. *The USA Patriot Act*

The USA Patriot Act altered the foreign intelligence surveillance framework in several important ways, with respect to scope, substantive standards and procedural provisions. First and most important, as discussed in further detail below, the Patriot Act altered the national security certification required for electronic surveillance and physical searches.[153] Rather than requiring a national security official to certify that "the purpose" of the surveillance was to obtain foreign intelligence information, the amended statute requires certification that "a *significant* purpose" of

---

that the information was "necessary for the conduct of an authorized foreign counterintelligence investigation," 15 U.S.C. § 1681u(a)-(b) (2000).

151. *See* 12 U.S.C. § 3414(a)(5)(A); 15 U.S.C. § 1681u(a)(2) (2000); 18 U.S.C. § 2709(b)(1) (2000).

152. Each of the NSL authorities contained a "gag" provision prohibiting the entity from which the records were sought from disclosing "to any person" that the FBI has sought or obtained access to information or records under the provision. *See* 12 U.S.C. § 3414(a)(5)(D); 15 U.S.C. § 1681u(d); 18 U.S.C. § 2709(c). A district court held that the NSL provision concerning transactional records held by a wire or electronic communications provider was unconstitutional after concluding that the provision did not permit a provider to consult with an attorney to challenge the NSL demand. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 506 (S.D.N.Y. 2004).

153. *See infra* notes 178-98 and accompanying text.

the surveillance or search is to obtain foreign intelligence information.[154] The Patriot Act also altered certain procedural aspects of FISA coverage for electronic surveillance and physical searches. In particular, the Patriot Act extended the period of approval for physical searches from forty-five days to ninety days.[155] For both electronic surveillance and physical searches, the Patriot Act permitted approval of a surveillance or search targeting an officer or employee of a foreign power or a member of a terrorist group for up to 120 days, and for a renewal period of up to one year.[156]

In addition to these changes to FISA's electronic surveillance and physical search coverage, the Patriot Act made some significant changes to the "lesser" foreign intelligence authorities described above. First, for pen register and trap-and-trace authority as well as for business records authority, the Patriot Act eliminated the requirement that officials link the information sought to a foreign power or an agent of a foreign power. Each type of order may now be granted upon a showing that the information likely to be obtained is "foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[157] If the investigation concerns a U.S. person, it cannot be conducted "solely upon the basis of activities protected by the first amendment to the Constitution."[158] Second, with respect to business records authority, the Patriot Act dramatically changed the scope of the provision: the provision is no longer limited to travel-related records. Instead, the order can run to "any person" for production of records *or tangible things*.[159]

Finally, with respect to the various NSL authorities, the Patriot Act eliminated the requirement to link the records to a foreign power or agent of a foreign power, allowing a request solely upon a showing of relevance to a foreign counterintelligence investigation.[160] With the exception of the changes to the NSL authorities, all of these changes are set to expire via a sunset provision on December 31, 2005.[161]

---

154. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (Supp. I 2001)) (emphasis added).

155. USA Patriot Act § 207(a)(2), 115 Stat. at 282; *see* 50 U.S.C. § 1824(d)(2) (Supp. I 2001).

156. USA Patriot Act § 207(b)(2), 115 Stat. at 282; *see* 50 U.S.C. §§ 1805(e)(1), 1824(d)(2) (Supp. I 2001).

157. USA Patriot Act § 214(a)(2), 115 Stat. at 286; *see* 50 U.S.C. §§ 1842(c)(2), 1861(b)(2) (Supp. I 2001).

158. USA Patriot Act § 214(a)(2), 115 Stat. at 286.

159. *Id.* § 215, 115 Stat. at 287; *see* 50 U.S.C. § 1861 (Supp. I 2001).

160. USA Patriot Act § 505, 115 Stat. at 365; *see* 12 U.S.C. § 3414(a)(5)(A) (Supp. I 2001); 15 U.S.C. § 1681u(a)-(c) (Supp. I 2001); 18 U.S.C. § 2709 (2000 & Supp. I 2001).

161. *See* USA Patriot Act § 224, 115 Stat. at 294.

It is, of course, impossible to fully assess all of the shifts in the foreign intelligence surveillance framework between 1978 and 2001 and in the Patriot Act without exploring the investigative challenges that prompted them; assessing how the Fourth Amendment applies to the "main" FISA authorities (for electronic surveillance and physical searches), as well as to the "lesser" FISA authorities (for pen registers and trap-and-trace devices and tangible things) and to the NSL authorities; and comparing the foreign intelligence surveillance authorities to analogous criminal law tools. My discussion of FISA's gradual expansion is therefore not intended to suggest that the pre-Patriot Act and post-Patriot Act changes were unwarranted. It is readily apparent, however, that the foreign intelligence surveillance framework has moved in important ways away from the 1978 compromise recognizing the government's power to use a single investigative tool in relatively narrow circumstances.

The next two Parts explore one aspect of the shift away from the narrow 1978 framework: the failure of FISA's information structure to keep pace with the statutory changes.

III. THE (LIMITED) JUDICIAL ROLE IN THE FOREIGN INTELLIGENCE SURVEILLANCE FRAMEWORK

As explained in Part II, one goal of FISA was to interpose a judicial magistrate to make a (modified) probable cause determination before surveillance to gather foreign intelligence information could proceed. Because the role of the FISC is somewhat analogous to that of a judge or magistrate authorizing a Title III order or a search warrant, it is easy to assume that, in foreign intelligence investigations, courts—the FISC and others—will play a major role in evaluating the foreign intelligence surveillance framework, and in particular in testing the legality of surveillance and searches under the Fourth Amendment. Judicial involvement in foreign intelligence matters, however, differs in significant ways from judicial involvement in ordinary criminal matters. Courts other than the FISC rarely consider FISA issues; they tend to be highly deferential toward the FISC when they do; and the absence of any significant body of law in the area makes the issues that courts do face seem indeterminate, and thus particularly unsuited to searching judicial review.

None of this necessarily calls the foreign intelligence surveillance framework into question as a constitutional or policy matter, for the FISC judge's probable cause evaluation may adequately address the Fourth Amendment and other concerns. A defense of the foreign intelligence surveillance framework that relies wholly on the role of the FISC, however, overlooks the fact that the significance of a court decision lies not only in the substantive result it reaches, but also in its public articulation of legal norms. The secrecy surrounding the FISC disables its decisions from performing the latter function. The infrequency with which FISA issues arise in other courts, and the degree of deference afforded the FISC when they

do, means that publicly available court decisions will yield little information about how well the foreign intelligence surveillance framework balances privacy and security interests, and about the extent to which implementation of the statute comports with congressional intent. As I will argue, in enacting FISA in 1978, Congress seemingly recognized that fact and placed privacy safeguards and information-generating mechanisms outside of the judiciary. But relatively little attention has been paid to these mechanisms as the statutory framework has evolved.

This Part explores the judicial role in the foreign intelligence surveillance framework in greater detail. The framework has always raised difficult Fourth Amendment questions, and any major change to the framework will reinvigorate the debate over FISA's constitutionality. For various reasons, courts have largely deferred to Congress in its assessment of the constitutionality of FISA and to the FISC in its application of FISA. Using the lone wolf amendment as an example, I suggest that this practice is quite likely to continue, despite the important changes to the foreign intelligence surveillance framework described in Part II.

A. *Judicial Deference Regarding FISA's Constitutionality and Implementation*

As discussed in Part II.B, the substantive predicate for a FISA order differs in important ways from that required for a criminal search warrant or for a surveillance order under Title III. Moreover, FISA's procedural protections are less rigorous than those that apply to a criminal search warrant or a Title III order. We might therefore expect courts to closely measure the foreign intelligence surveillance framework against Fourth Amendment requirements and to scrutinize application of the statutory requirements (particularly those that may be constitutionally mandated). The secrecy surrounding the FISC process largely shields the FISC's application of statutory requirements from public view. Other courts have tended to adopt a deferential posture concerning FISA and its application. This section explores relevant pre-Patriot Act decisions to set the stage for an inquiry into how courts are likely to handle Fourth Amendment challenges to such changes as the lone wolf amendment.

A court recognizing the differences between foreign intelligence surveillance and searches and criminal surveillance and searches might address the Fourth Amendment implications of these differences (if any) in one of two ways. First, the court might consider whether a FISA order, despite the ways in which it differs from a criminal search warrant or Title III order, nevertheless constitutes a "warrant" for purposes of the Fourth Amendment. Alternatively, a court might examine whether the Fourth Amendment permits an exception to the warrant requirement in the sorts of cases in which FISA coverage is available, and whether FISA's alternative structure is reasonable.[162]

162. These two approaches, of course, can overlap. For example, if a court were to proceed from the premise that the Fourth Amendment's warrant require-

At least in evaluating FISA's pre-Patriot Act structure, courts have mainly taken the second approach. As noted, even after the Supreme Court's decision in *Keith*, three courts of appeals upheld warrantless surveillance to gather foreign intelligence information.[163] Carrying these decisions over into the FISA context, several courts assumed or held that the executive power to conduct foreign affairs exempts the Executive from the warrant requirement in gathering foreign intelligence information.[164] Recognizing that any search or seizure must still be reasonable, the courts evaluated whether, consistent with *Keith*, the standards for a FISA order were "reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens."[165] Courts uniformly found that the structure FISA set up satisfies this standard.

The decision that most fully explores the reasonableness of FISA's procedures is that of the Court of Appeals for the Second Circuit in 1984 in *United States v. Duggan*.[166] The *Duggan* court drew upon the Supreme Court's discussion of domestic security surveillance in *Keith* and upon the Senate Select Committee on Intelligence report accompanying FISA[167] to highlight a number of differences between ordinary criminal investigations and foreign intelligence investigations. The differences the *Duggan* court identified can be usefully categorized to include: (1) the *heightened interest* of the United States in protecting against hostile acts of foreign powers, particularly in light of the nation's "'international responsibilities;'"[168] (2) the fact that intelligence gathering serves different *goals*—

---

ment is sufficiently flexible to permit the necessary showings to differ depending upon the government interests at stake, then its conclusion that a FISA order is a warrant would be indistinguishable from a conclusion that FISA's structure is reasonable. *See, e.g.*, United States v. Megahey, 553 F. Supp. 1180, 1190, 1192 (S.D.N.Y. 1982) (considering whether FISA order is warrant within meaning of Fourth Amendment; concluding that differences between FISA orders and criminal warrants are "reasonably adapted to the peculiarities of foreign intelligence gathering"), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

163. *See supra* notes 73-74 and accompanying text.

164. *See, e.g.*, United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (observing that, prior to enactment of FISA, "this court joined all save one of the circuits to have addressed the question in holding that the President has the inherent power to conduct warrantless electronic surveillance for foreign intelligence purposes"); *Duggan*, 743 F.2d at 72-73 (noting courts' widespread conclusions prior to FISA's passage that foreign intelligence surveillance constituted exception to warrant requirement, and considering whether FISA's procedures adequately balance interests at stake); United States v. Falvey, 540 F. Supp. 1306, 1312 (S.D.N.Y. 1982) (concluding that "the executive power to conduct foreign affairs exempts the President from the warrant requirement when foreign surveillance is conducted").

165. *Keith*, 407 U.S. 297, 323 (1972) (citing Camara v. Municipal Court, 387 U.S. 523, 534-35 (1967)).

166. 743 F.2d at 59.

167. *See* S. REP. NO. 95-701 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973.

168. *Duggan*, 743 F.2d at 73 (quoting S. REP. NO. 95-701, at 14-15, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983).

prevention and preparedness, rather than accumulation of evidence—than does surveillance in ordinary criminal cases;[169] (3) the need to maintain *secrecy* of counterintelligence sources and methods;[170] and (4) a range of *logistical challenges* presented by investigating hostile activities of foreign powers. With respect to these logistical challenges, the *Duggan* court's reliance on *Keith* and the SSCI report revealed several: (a) that intelligence gathering can involve reliance on "'the interrelation of various sources and types of information;'"[171] (b) that it may be more difficult to identify an exact target, with the result that the necessary showings will have to be "'less precise'" than in the case of "'more conventional types of crime;'"[172] and (c) that, where activities of "'foreign intelligence services and foreign-based terrorist groups'" are involved, those activities may have been "'planned, directed, and supported abroad.'"[173]

The *Duggan* case concerned international terrorism, and the Second Circuit, like other courts, emphasized the government's compelling need to obtain foreign intelligence relating to such activities.[174] The *Duggan* court also directly addressed a challenge to FISA's requirement to show only "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power," not probable cause that the target has committed a crime.[175] The court concluded that FISA's adjusted probable cause finding is properly tailored to foreign intelligence gathering, and that interposing a judicial magistrate to make that finding serves as an effective control on arbitrary governmental conduct and a fundamental safeguard for individual liberty.[176] All courts that have addressed Fourth Amendment challenges to the pre-Patriot Act FISA, both before and after *Duggan*, have agreed.[177]

---

169. *Id.* at 72 (noting emphasis of intelligence gathering on "'prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency'" (quoting *Keith*, 407 U.S. at 322-23)).

170. *Id.* at 73 (noting "'need to maintain the secrecy of lawful counterintelligence sources and methods'" (quoting S. REP. NO. 95-701, at 14-15, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983)).

171. *Id.* at 72 (quoting *Keith*, 407 U.S. at 322-23).

172. *Id.* (quoting *Keith*, 407 U.S. at 322-23).

173. *Id.* at 73 (quoting S. REP. NO. 95-701, at 14-15, *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983).

174. *See id.* at 74 ("We find highly persuasive the conclusions of Congress and the executive branch . . . that international terrorist organizations are legitimate and important targets for foreign intelligence surveillance."); *see also* United States v. Falvey, 540 F. Supp. 1306, 1312 (S.D.N.Y. 1982) ("No one can gainsay that obtaining foreign intelligence relating to international terrorism is a legitimate object of the Executive's constitutional authority to conduct foreign policy.").

175. *See* 50 U.S.C. § 1805(a)(3)(A) (2000).

176. *Duggan*, 743 F.2d at 73 (concluding that required judicial findings "provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment").

177. *See* United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (noting that "FISA requires judicial review prior to the initiation of the type of surveillance

From a doctrinal perspective, it is difficult to assail these conclusions. Courts have simply viewed FISA as fitting into the opening left by the *Keith* case. From a normative perspective, one could argue that FISA reflected a compromise between national security and privacy interests at a crucial moment of political awareness of abuses of executive power. In this context, the participants' views of FISA's constitutionality should be afforded some deference. Indeed, the inherent indeterminacy of *Keith*'s "reasonableness" inquiry makes it difficult for courts not to defer to Congress's assessment of the statute's constitutionality.

I have thus far considered only the deference courts tend to give to Congress's assessment of FISA's constitutionality. Courts have similarly afforded a great deal of deference to FISC judges' application of FISA in individual cases. Because notice of a FISA surveillance or search typically occurs only when a government entity seeks to introduce evidence in a judicial or other proceeding, courts other than the FISC evaluate only a small percentage of FISA applications. No court has ever concluded that a FISA order was improperly issued.

B. *Challenges to Judicial Deference?*

As the analysis in Section A suggests, courts (other than the FISC) have played only a limited role in the development and articulation of law under FISA. One might question whether this limited role is likely to persist in the face of the important changes to the statutory scheme, such as the Patriot Act's "significant purpose" language and the lone wolf amendment. If we view FISA as passed in 1978 as reflecting the participants' shared understanding of the contours of the Fourth Amendment in the foreign intelligence context, then we might regard FISA's standards as quasi-constitutional. The "significant purpose" and lone wolf changes each undermine aspects of the FISA compromise. In addition, because the "significant purpose" change is likely to result in greater use of FISA in cases that ultimately result in criminal proceedings, we are likely to see increased consideration of FISA's application in ordinary courts. With respect to both changes, however, courts will likely be faced with the same problems of indeterminacy as courts evaluating earlier versions of FISA. Continued deference to Congress and the FISC, especially with respect to the lone wolf provision, is the likely result. This section explains why.

---

conducted here and sets careful limitations on its exercise," including by requiring probable cause to believe that target is agent of foreign power); United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (observing that "the showing necessary under the Fourth Amendment to justify a surveillance conducted for national security purposes is not necessarily analogous to the standard of probable cause applicable to criminal investigations;" concluding that "the probable cause showing required by FISA is reasonable"); *Falvey*, 540 F. Supp. at 1313 ("[T]he FISA probable cause standard fully satisfies the Fourth Amendment requirements as construed by the *Keith* Court."); *see also* United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991) (following *Duggan*; rejecting argument that FISA violates prohibition on warrantless searches).

To understand the constitutional issues surrounding the Patriot Act's "significant purpose" language, it is essential to appreciate the institutional issues that led to its enactment. The change was prompted by concern about the adoption and implementation of Attorney General Guidelines concerning the sharing of FISA-derived information between counterintelligence and criminal investigators and prosecutors within the FBI and the Justice Department.[178] As implemented, the Guidelines greatly restricted the exchange of FISA-derived information.[179] The Guidelines were adopted in part out of concern that the FISC would deny FISA renewal requests or another court would disallow use of FISA-derived evidence in cases in which criminal investigators and prosecutors were too heavily involved.

This focus on the level of involvement of criminal investigators and prosecutors can be traced to a pre-FISA case, *United States v. Humphrey*[180] (appealed as *United States v. Truong Dinh Hung*[181]), in which a district court concluded that warrantless surveillance was unlawful once the gathering of foreign intelligence information was not the "primary purpose" of the surveillance.[182] The court identified the point at which the "primary purpose" had shifted to criminal prosecution by conducting an evidentiary hearing to assess the involvement of criminal prosecutors in the case.[183] Without specifically addressing the district court's methodology in determining when the shift in the investigation's primary purpose had occurred, the Court of Appeals for the Fourth Circuit affirmed.[184]

As enacted, FISA required certification by a national security official that "*the* purpose" of the surveillance was to obtain foreign intelligence information.[185] Drawing upon *Humphrey/Truong*, however, defendants challenging FISA surveillance maintained that such surveillance could only proceed where "the *primary* purpose" of the surveillance was to obtain foreign intelligence information. The only court to consider directly

178. *See* Memorandum from Janet Reno, Attorney General, to Assistant Attorney General, Criminal Division; Director, FBI; Counsel for Intelligence Policy; and United States Attorneys, *Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations* (July 19, 1995), *at* http://?www.fas.org/?irp/?agency/doj/fisa/1995procs.html (last visited April 7, 2005).

179. *See, e.g.*, ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION, FINAL REPORT 707-52 (2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows.htm (last visited April 7, 2005) [hereinafter BELLOWS REPORT]; GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 11-15 (2001) [hereinafter GAO COORDINATION REPORT].

180. 456 F. Supp. 51 (E.D. Va. 1978).

181. 629 F.2d 908 (4th Cir. 1980).

182. *See Humphrey*, 456 F. Supp. at 59.

183. *Id.*

184. *Truong*, 629 F.2d at 915.

185. 50 U.S.C. § 1804(a)(7)(B) (2000) (emphasis added).

whether the pre-FISA "primary purpose" test should be imported into FISA questioned whether that test should apply,[186] and the decision was not appealed. A series of court of appeals decisions soon invoked the primary purpose test in upholding FISA surveillance.[187] Because all of the cases involved explicit or implicit conclusions that the primary purpose of the surveillance was in fact to gather foreign intelligence information, no court actually had to consider whether to apply a different standard.[188] Nor did any court directly consider precisely what might convert surveillance from one primarily directed at gathering foreign intelligence information to one primarily directed at gathering evidence for a criminal prosecution. In this context, the Attorney General Guidelines were essentially prophylactic—designed to prevent the sort of contacts within the Justice Department that might trigger a court's conclusion that the primary objective of the surveillance was not to gather foreign intelligence information.

By shifting the required certification from "the purpose" to "a significant purpose," Congress sought to eliminate the sort of strict separation between counterintelligence and criminal investigators and prosecutors that the Attorney General Guidelines had apparently fostered.[189] But the change necessarily reopens the seemingly settled question of FISA's constitutionality under the Fourth Amendment. First, to the extent that courts have recognized a foreign intelligence exception to the Fourth Amendment's warrant requirement, the question is whether that exception should apply where the gathering of foreign intelligence information is not the main purpose of the surveillance or search. Second, in applying *Keith*'s directive to assess the reasonableness of FISA's procedures in rela-

186. *See* United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982) ("What the defendants steadfastly ignore . . . is that in this case—unlike *Truong*—a court order was obtained authorizing the surveillance. . . . An order authorizing the surveillance in this case was lawfully obtained pursuant to FISA. Accordingly, all the relevant evidence derived therefrom will be admissible at trial.").

187. *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1992) ("Although evidence obtained under FISA subsequently may be used in criminal prosecutions . . ., the investigation of criminal activity cannot be the primary purpose of the surveillance.") (citing *Truong*, 629 F.2d at 915); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) (finding in FISA "[t]he requirement that foreign intelligence information be the primary objective of the surveillance"); *see also* United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987) ("We agree with the district court that 'the primary purpose of the surveillance, both initially and throughout, was to gather foreign intelligence information.'"); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (declining to suppress surveillance evidence where surveillance "did not have as its purpose the primary objective of investigating a criminal act"); *cf.* United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987) (stating that "the purpose of the surveillance, both as proposed and actually conducted, was to secure foreign intelligence information and not to aid in criminal investigations").

188. *See Johnson*, 952 F.2d at 572; *Pelton*, 835 F.2d at 1075-76; *Badia*, 827 F.2d at 1464; *Duggan*, 743 F.2d at 77-78.

189. For discussion of this strict separation, see BELLOWS REPORT, *supra* note 179, at 707-52; GAO COORDINATION REPORT, *supra* note 179, at 11-15.

tion to the government interest at stake and the rights of individuals, courts have measured whether FISA's probable cause standard was properly adapted to the peculiarities and complexities of foreign intelligence gathering—an inquiry that seems less appropriate when foreign intelligence gathering is not the principal purpose of FISA coverage.

Whether the shift to the Patriot Act's "significant purpose" is constitutional remains an open question. In its first ever decision, the Foreign Intelligence Surveillance Court of Review (FISCR)—the panel created to adjudicate appeals from denials of FISA applications—has concluded that the change is constitutional, at least when construed to permit use of FISA where the primary purpose of the surveillance or search is to obtain evidence of foreign intelligence crimes (as distinct from ordinary crimes).[190] The FISCR nevertheless acknowledged that "the constitutional question presented by this case . . . has no definitive jurisprudential answer."[191] Other challenges to the "significant purpose" language are underway.[192] The courts considering those challenges are not bound by the FISCR decision but, if past practice is any indication, they are likely to give that decision a strong degree of deference.

The lone wolf amendment adds another layer of complexity to this Fourth Amendment analysis. The amendment essentially alters the probable cause showing that must be made to secure FISA coverage in lone wolf cases by eliminating (in the case of a non-U.S. person) the requirement to demonstrate that the target's activities are conducted "on behalf of a foreign power." Recall that FISA requires the FISC to find probable cause to believe that the target of the surveillance or search is a "foreign power" or an "agent of a foreign power." Although the lone wolf amendment does not eliminate that requirement, it nevertheless allows approval of FISA coverage without any evidence linking a target's activities to a foreign power, because the amendment permits a target to be treated as an "agent" of a foreign power when "agency" in the typical sense cannot be shown. As in other contexts, a court is likely to evaluate the change by focusing on, first, whether use of the amended provision would fall within the foreign intelligence exception to the warrant requirement, and, second, whether FISA's procedures are reasonable in this context.

190. *See In re* Sealed Case, 310 F.3d 717, 736, 746 (Foreign Intel. Surv. Ct. Rev. 2002).

191. *Id.* at 746.

192. For one example, see Second Amended Motion for Disclosure of Materials Related to Surveillance Pursuant to the Foreign Intelligence Surveillance Act (FISA) and for Suppression of the Fruits of All Surveillance Conducted Under FISA and Memorandum of Law in Support at 29-35, United States v. Hatem Naji Fariz (No. 8:03-CR-77-T-30TBM) (M.D. Fla. filed Nov. 24, 2004), *at* http://www.flmd.uscourts.gov/al-arian/8-03-cr-00077-JSM-TBM/docs/ 1663751/0.pdf (last visited Apr. 7, 2005). The district court deemed the defendants' arguments "foreclosed" by the FISCR's decision. United States v. Sami Amin al-Arian, No. 8:03-CR-77-T-30TBM, slip op. at 14 n.9 (M.D. Fla. Apr. 19, 2005), *at* http://www.flmd.uscourts.gov/Al-Arian/8-03-cr-00077-JSM-TBM/docs/2066202/0.pdf (last visited Sep. 2, 2005). The decision has not yet been appealed.

On the first point, it is important to recall that the *Keith* Court, in emphasizing the narrowness of its opinion, carved out only those cases involving foreign powers and their agents.[193] Again, the lone wolf amendment does not eliminate the statutory requirement to demonstrate probable cause that the target is an "agent of a foreign power," but it does allow the FISC to make that finding without so much as a hint of a link to a foreign power. Even FISA's definition of foreign intelligence information presumes this link between a target's activities and a foreign power: with respect to the counterintelligence category,[194] the definition includes only information relating to the United States' ability to protect against those activities undertaken by "a foreign power or an agent of a foreign power."[195] FISA's definition of foreign intelligence information of course need not necessarily match the contours of a foreign intelligence exception to the Fourth Amendment's warrant requirement. It is worth noting, however, that in a pre-FISA case involving surveillance to gather foreign intelligence information, but where the targets of the surveillance were not agents of a foreign power, the Court of Appeals for the D.C. Circuit, sitting en banc, held that the government's conduct violated the Fourth Amendment.[196] The Senate Judiciary Committee report accompanying FISA discussed the case[197] and reflected the view that a link between the surveillance target and a foreign power was important to the constitutionality of the statutory scheme.[198]

Whether the requirements for FISA coverage of a lone wolf are "reasonable"—in light of the governmental interest at stake and the nature of the intrusion—also presents a difficult question. As noted, in assessing the reasonableness of FISA's structure, courts have relied heavily on the requirement to link a target's conduct to a foreign power or agent of a for-

193. *See supra* notes 66-67 and accompanying text.

194. *See* 50 U.S.C. § 1801(e)(1) (2000); *supra* notes 89-93 and accompanying text.

195. More specifically, the definition includes information concerning the ability of the United States to protect against "actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;" "sabotage or international terrorism by a foreign power or an agent of a foreign power;" or "clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." 50 U.S.C. § 1801(e)(1).

196. *See* Zweibon v. Mitchell, 516 F.2d 594, 614 (D.C. Cir. 1975) (en banc) (plurality opinion) ("[W]e hold today . . . that a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power, even if the surveillance is installed under presidential directive in the name of foreign intelligence gathering for protection of the national security."); *id.* at 689 (Wilkey, J., concurring in part and dissenting in part) (agreeing with plurality that if exemption from warrant requirement exists, "it exists only for a narrow category of wiretaps on foreign agents or collaborators with a foreign power").

197. S. REP. No. 95-694 pt. 1, at 15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916.

198. *See id.* at 16, *reprinted in* 1978 U.S.C.C.A.N. at 3917 (noting limitation of statute to foreign powers and agents of foreign powers).

eign power, concluding that this requirement provides an adequate substitute for a showing of probable cause that a specific crime has been committed.[199]

In addition, in upholding the Patriot Act's "significant purpose" change, the FISCR specifically acknowledged the importance of linking the target's conduct to a foreign power. The FISCR upheld the significant purpose change in part because it perceived FISA to apply "only to certain carefully delineated, and particularly serious, foreign threats to national security."[200] In support of that conclusion, the FISCR explained why FISA surveillance "would not be authorized against a target engaged in purely domestic terrorism": because "the government *would not be able to show that the target is acting for or on behalf of a foreign power.*"[201] Although the FISCR used the example of domestic terrorism rather than international terrorism, the FISCR clearly regarded the requirement of a link to a foreign power as crucial to the statutory scheme.

The "reasonableness" of the probable cause showing required for lone wolf cases turns in part on whether an "ordinary" probable cause determination would suffice in such cases. It is instructive to consider again the discussions in *Keith* and *Duggan* concerning the differences between security surveillance and surveillance of ordinary crime: differences with respect to the government interest involved, the goals of the surveillance, the secrecy required and the logistical challenges (as to the interrelationship of sources, precision with respect to the target and the practical problems involved where activities are planned and conducted abroad).

One argument for the unreasonableness of lone wolf surveillance might be that, when a judge must consider only the activities of a single individual to find probable cause, some of the factors distinguishing security surveillance from surveillance of ordinary crime—particularly the investigative challenges—do not apply. When the acts of a single individual form the basis of the probable cause determination, that determination is less likely to involve "interrelation of various sources and types of information."[202] The exact target of the surveillance, moreover, is not difficult to identify. And to the extent that the government might be using the lone wolf amendment where foreign intelligence gathering is not the central purpose of the investigation—a scenario that the Patriot Act clearly permits—the goals of the investigation might not differ from those in an ordinary criminal investigation. At the same time, because FISA would still require a showing of activities in preparation for international terrorism—a term defined to include acts that "occur totally outside of the United States, or transcend national boundaries"[203]—a lone wolf investigation

199. *See supra* notes 175-76 and accompanying text.

200. *In re* Sealed Case, 310 F.3d 717, 739 (Foreign Intel. Surv. Ct. Rev. 2002).

201. *Id.* (emphasis added).

202. *Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (quoting *Keith*, 407 U.S. 297, 322-23 (1972)).

203. 50 U.S.C. § 1801(c)(3) (2000).

would still involve "the difficulties investigating activities planned, directed, and supported from abroad."[204]

In short, as with the "significant purpose" change in the Patriot Act, there is no "definitive jurisprudential answer" to the constitutional question the lone wolf amendment raises.[205] In light of the weight of precedent upholding FISA in its original form, and the fact that at least some of the factors supporting the reasonableness of FISA as enacted also support the lone wolf amendment, it seems unlikely that a court (either the FISC itself, or a federal court considering a challenge to FISA-derived evidence) would invalidate use of the lone wolf authorization on Fourth Amendment grounds.

In predicting that a court would likely uphold the lone wolf amendment as consistent with the Fourth Amendment, I do not intend to suggest that a full normative analysis would yield the same result. The normative picture is also quite complicated. On the one hand, the lone wolf amendment applies only to non-U.S. persons (i.e., persons who are neither citizens nor permanent resident aliens) and does not disturb the requirement to show that the target is engaged in activities in preparation for terrorism. On the other hand, if the Fourth Amendment applies within the United States to U.S. persons and non-U.S. persons alike,[206] it is unclear why the lone wolf amendment's focus on non-U.S. persons makes the provision any more constitutional than it otherwise might be. In addition, the limiting effect of the requirement to show that the target is engaging in activities in preparation for international terrorism is highly dependent on how broadly the "in preparation" phrase is construed. Moreover, if FISA's original substantive standards should be treated as quasi-constitutional, then

204. *Duggan*, 743 F.2d at 73 (quoting S. REP. No. 95-701, at 14-15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3983).

205. *In re* Sealed Case, 310 F.3d at 746.

206. The Supreme Court has never explicitly held that nonresident aliens within the United States are entitled to Fourth Amendment protection. In *INS v. Lopez-Mendoza*, 486 U.S. 1032 (1984), the Court considered on the merits Fourth Amendment claims by illegal aliens, but did not explicitly hold that the Fourth Amendment applied. *See also* United States v. Verdugo-Urquidez, 494 U.S. 259, 272 (1990) (noting that "[o]ur statements in Lopez-Mendoza are therefore not dispositive of how the Court would rule on a Fourth Amendment claim by illegal aliens in the United States if such a claim were squarely before us"). Both before and after *Lopez* and *Verdugo*, courts of appeals have held or assumed that the Fourth Amendment does apply to nonresident aliens within the United States. *See, e.g.*, *Duggan*, 743 F.2d at 75 (observing that "the Fourth Amendment and the Equal Protection Clause afford protection to all aliens"); Au Yi Lau v. INS, 445 F.2d 217, 223 (D.C. Cir. 1971) (observing that "aliens in this country are sheltered by the Fourth Amendment in common with citizens"); United States v. Guitterez, 983 F. Supp. 905, 916 (N.D. Cal. 1998) (holding, notwithstanding Court's decision in *Verdugo*, that Fourth Amendment applies to illegal aliens within United States), *rev'd on other grounds*, 203 F.3d 833 (9th Cir. 1999); *see also* Martinez Camargo v. INS, 282 F.3d 487, 493 (7th Cir. 2002) (evaluating whether illegal aliens' Fourth Amendment rights were violated); United States v. Rodriguez-Arreola, 270 F.3d 611, 617 (8th Cir. 2001) (same); Babula v. INS, 665 F.2d 293, 297 (3d Cir. 1981) (same).

any significant move away from those substantive standards should be closely scrutinized.

My point, then, is not that a court *should* not closely scrutinize the lone wolf amendment; it is that a court drawing upon available precedent is unlikely to find a surveillance or search unconstitutional where the predicates for lone wolf surveillance are met. That purely predictive point may say less about the substance of the lone wolf amendment than it does about the statutory and practical limits on judicial involvement in the FISA process, particularly in light of the relatively small number of cases in which use of FISA comes to light at all.

Although I have thus far considered only constitutional questions concerning the statutory framework itself—not questions concerning the legality under the Fourth Amendment (or FISA itself) of particular searches—similar observations concerning the judicial role still hold. Questions concerning the legality of particular searches arise relatively infrequently, and courts tend to defer to the FISC's assessment of whether statutory and constitutional standards are met. Although the secrecy surrounding the FISA process makes assessment difficult, there have been more than 17,000 FISA applications and renewals granted since 1979, and challenges to introduction of FISA-derived evidence have been brought in approximately twenty-one cases.[207] None of these challenges have been successful.[208]

Of course, the relative infrequency of post-surveillance judicial review of the FISA process does not mean that judicial involvement is absent: by all accounts, the FISC rigorously tests the applications brought before it to ensure that the appropriate standards are met. What it does mean, however, is that whatever body of "law" that exists on application of FISA is,

---

207. The number in the text reflects cases published in the national reporter system or available on Westlaw or Lexis. It includes sixteen cases in which a defendant in a criminal case moved to suppress FISA-derived evidence (including eleven cases in which a court of appeals affirmed denial of a suppression motion and five cases decided at the district court level and apparently not appealed), as well as five cases adjudicating the legality of a FISA surveillance or search in some other procedural posture (such as a civil suit, a request by the government for a declaratory judgment concerning the legality of the surveillance or a challenge referred to a U.S. district court concerning evidence sought to be used in a foreign proceeding). The figure does not include purely procedural dispositions, such as a determination that a party lacks standing to contest the legality of FISA's use. Although suppression is also quite rare in the Title III context, the sheer number of suppression motions under Title III makes tabulation and comparison impossible.

208. In one case, a district court noted that there were certain gaps between FISC orders authorizing electronic surveillance. The court therefore ordered suppression of any communication seized during these gaps, although it was unclear that any surveillance had actually occurred during the time periods in question. *See* United States v. Sami Amin al-Arian, No. 8:03-CR-77-T-30TBM, slip op. at 7-8 (M.D. Fla. Apr. 19, 2005), *at* http://www.flmd.uscourts.gov/Al-Arian/8-03-cr-00077-JSM-TBM/docs/2066202/0.pdf (last visited Sept. 2, 2005).

unlike in the criminal context, (almost) entirely shielded from public view.[209] The next Part explores the implications of this fact.

IV. RETHINKING FISA'S INFORMATION STRUCTURE

In Part III, I highlighted the limited judicial role in evaluating FISA and its application. The FISC, of course, is a central player in the FISA process, at least for requests for orders permitting electronic surveillance and physical searches. The involvement of a FISC judge as a judicial magistrate evaluating probable cause, however, does not result in any sort of public articulation of law. The limited involvement of other courts can therefore have significant consequences. At worst, courts' general posture of deference to Congress and to the FISC pretermits assessment of FISA's privacy implications by the branch that we most expect to engage in such assessment. At best, even if FISC judges' thorough scrutiny of FISA applications obviates the need for further judicial evaluation of FISA's privacy implications, the fact that all aspects of the FISC's assessment are shielded from public view deprives the public and Congress of the ordinary tools for evaluating the investigative powers granted to the Executive. In other words, without public judicial decisions generating information about FISA and its implementation, there are limits upon the public's and Congress's ability to assess FISA's privacy implications, and limits on the public's and Congress's ability to assess the Executive's and the FISC's fidelity to the statutory structure.

In this Part, I argue that maintaining a well-functioning—and publicly acceptable—framework for foreign intelligence gathering in the United States requires a careful focus on the mechanisms for generating information about the Executive's and the FISC's implementation of foreign intelligence surveillance law. At the time of the 1978 FISA compromise, Congress recognized that fact. As the foreign intelligence surveillance framework has shifted and expanded over nearly three decades, however, Congress's attention to the framework's "information structure" has been haphazard and episodic. Indeed, in passing the lone wolf amendment, Congress for the first time adopted uniform reporting requirements for all FISA authorities (though not for NSLs). As I will argue, however, further changes are necessary.

A. *The 1978 Compromise*

Part II.A discussed the political and constitutional context for FISA's passage in 1978. Congress sought both to recognize and to rein in an

209. The two notable exceptions are (1) the FISC order denying an application for authorization of a physical search, *see supra* note 131 and accompanying text; and (2) the FISC and FISCR opinions addressing the Justice Department's post-Patriot Act interpretation of FISA, *see In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002) (en banc); *In re* Sealed Case, 310 F.3d 717 (Foreign Intel. Surv. Ct. Rev. 2002).

executive power to engage in electronic surveillance activities to gather foreign intelligence information. The FISC was a crucial part of the resulting statutory scheme, but other courts arguably were not. To be sure, FISA required government entities to notify an "aggrieved person" of an intention to "enter into evidence or otherwise use or disclose" information "obtained or derived from an electronic surveillance of that aggrieved person" in a judicial or other proceeding,[210] and permitted such aggrieved person to move to suppress the evidence on the grounds that the information was "unlawfully acquired."[211] Congress also recognized, however, that in the vast majority of cases, investigators would not seek to introduce FISA evidence in a judicial or other proceeding.[212]

As suggested in Part III, the limited post-surveillance judicial review in the FISA process has two problematic consequences. First, it makes it less likely that courts other than the FISC will significantly shape the scope of the statute, thereby placing additional pressure on Congress to ensure that the statute adequately balances the competing privacy and security considerations and to ensure that the executive branch and the FISC are properly interpreting the statute. Second, limited post-surveillance review largely removes the FISA process from public view, thus making it difficult for the public to observe how widely and how well surveillance authorities are used. In other words, the absence of post-surveillance review raises concerns about substantive outcomes (systemically and at the level of individual cases) as well as legitimacy.

Recognizing that post-surveillance judicial review in individual cases would be rare, Congress sought in two other ways to ensure that FISA was properly used. First, Congress required that a detailed executive review occur before an application was even presented to the FISC.[213] The detailed requirements no doubt contributed to the institutional evolution within the Justice Department, with the eventual emergence of the Office of Intelligence Policy and Review as the gatekeeper to the FISC. Although the requirements were designed as a privacy protection mechanism to ensure FISA's proper use, they were not necessarily designed to contribute to public or congressional evaluation of FISA's use. But Congress also imposed certain public and inter-branch reporting requirements, and specifically contemplated that these requirements would facilitate the oversight that would be necessary in the absence of routine judicial review.[214]

---

210. 50 U.S.C. § 1806(c)-(d) (2000).

211. *Id.* § 1806(e).

212. *See* S. REP. NO. 95-701, at 657 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4036 ("[U]nlike the statutory provisions of Title III of the Omnibus Crime Control Act of 1968, it is not contemplated that most electronic surveillance conducted pursuant to this chapter will result in criminal prosecution.").

213. 50 U.S.C. § 1804 (2000); *see* S. REP. NO. 95-604 pt. 1, at 16, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3917-18 (describing "internal" check on Executive).

214. *See* S. REP. NO. 95-604 pt. 1, at 60 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3961-62; S. REP. NO. 95-701, at 66-67 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4035-36.

The statute required the Attorney General to transmit to the Administrative Office of United States Courts and to Congress reports setting forth "the total number of applications made for orders and extensions of orders approving electronic surveillance" under FISA and "the total number of such orders and extensions either granted, modified, or denied."[215] The statute also required the Attorney General to "fully inform" the congressional intelligence committees "concerning all electronic surveillance" under FISA.[216] Finally, Congress also required the intelligence committees, for five years after FISA's enactment, to report to their respective chambers concerning implementation of the statute, including whether FISA should be amended, repealed or permitted to continue in effect.[217] All of these reports were made public.[218]

We can view the public and congressional reporting requirements as serving two functions under FISA. First, even the statistical reporting requirement can serve a privacy protective function, insofar as it can reveal the extent of FISA's use (or abuse) and drive a congressional response. Second, if properly implemented, the more detailed committee reporting requirements to some extent compensate for the absence of significant judicial interpretations of the statute. Such requirements allow both for the evaluation of FISA's privacy implications and for the evaluation of the Executive's and the FISC's fidelity to congressional intent. In other words, the requirements act as a check on the FISA process—albeit at a systemic level rather than in individual cases.

B. *Neglect of FISA's Information Structure*

Part II.C described several shifts in FISA's scope and substantive standards. As substantive changes occurred on a piecemeal basis, Congress to some extent mirrored the reporting requirements accompanying the electronic surveillance provisions. Those requirements, however, were narrowly interpreted by the executive branch. And until quite recently, Congress gave no consideration to whether the shifts in FISA's substantive coverage necessitate more structured oversight. Congress finally adopted broader reporting requirements in the recent lone wolf amendment, but there is good reason to be skeptical that the new requirements will dramatically alter FISA's information structure.

---

215. 50 U.S.C. § 1807 (2000).

216. *Id.* § 1808(a).

217. *Id.* § 1808(b).

218. *See* S. REP. NO. 98-660 (1984); H.R. REP. 98-738 (1984); S. REP. NO. 97-691 (1982); H.R. REP. 97-974 (1982); S. REP. NO. 97-280 (1981); H.R. REP. 97-318 (1981); S. REP. NO. 96-117 (1980); H.R. REP. NO. 96-1466 (1980); S. REP. NO. 96-379 (1979); H.R. REP. NO. 96-558 (1979).

1. *Public Reporting of Statistical Information*

In FISA as passed in 1978, Congress required that information about the total number of electronic surveillance applications requested and granted, modified or denied be transmitted to the Administrative Office of the United States Courts.[219] In doing so, Congress tracked one aspect of the requirements that apply to surveillance under Title III.[220] Like the statistical reports required under Title III, the reports on electronic surveillance under FISA have always been publicly released. Statistical reporting requirements added in subsequent FISA amendments have not mentioned the Administrative Office, thus leaving the Executive freer to interpret the requirements to permit reporting in a classified committee setting. In the 1994 physical search amendment, for example, Congress included a requirement that the Attorney General report to the Judiciary Committees, on a semiannual basis, the total number of physical search applications requested and granted, modified or denied, as well as the number of physical searches that involved property of United States persons.[221]

The 1998 FISA amendments, adding pen register and trap-and-trace authority and authority to compel production of business records, likewise contained a requirement to provide the Judiciary Committees with statistical information.[222] The Justice Department has apparently interpreted the 1994 and 1998 requirements not to mandate any public reporting, because it does not provide any public statistics specifically concerning physical searches, pen registers and trap-and-trace devices, or business records. The Department does, however, include in its report to the Administrative Office the total number of physical search orders, aggregated along with the electronic surveillance statistics.[223] Because the only requirement the Justice Department cites in submitting those reports is the requirement applying to electronic surveillance,[224] it is unclear why the Department believes that statistics on physical searches can or should be aggregated with statistics on electronic surveillance. The Department does not similarly aggregate pen register or trap-and-trace or business records statistics, despite the parallel statutory language in the 1994 and 1998 amendments. The Justice Department has refused to release pen/trap and business records statistics in any non-classified setting.[225]

219. *See* 50 U.S.C. § 1807.

220. *See* 18 U.S.C. § 2519(2) (2000).

221. *See* 50 U.S.C. § 1826.

222. *See id.* §§ 1846(b), 1863(b) (repealed 2001); *see also* 50 U.S.C. § 1862 (Supp. I 2001).

223. *See, e.g.*, Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, U.S. Dep't of Justice, to L. Ralph Mecham, Director, Administrative Office of United States Courts (Apr. 30, 2004), *at* http://?www.usdoj.gov/?oipr/?readingroom/?2003fisa-ltr.pdf (last visited Apr. 7, 2005).

224. *Id.*

225. *See, e.g.*, Declaration of James A. Baker, Counsel for Intelligence Policy, at 6-7, American Civil Liberties Union v. U.S. Dep't of Justice, Civ. Action No.

As this discussion suggests, despite the expansion of the foreign intelligence surveillance framework, Congress has paid little attention to public reporting requirements, allowing the single requirement for a report to the Administrative Office concerning electronic surveillance to bear the weight of the expanding statutory framework. And unsurprisingly, the national security letter authorities enacted in 1986 and 1996 contain no public reporting requirements whatsoever. Freedom of Information Act requests for information concerning use of NSL authorities have resulted in no information on the individual or aggregate use of these authorities; the FBI instead has released a "list" of NSLs with all substantive information redacted, and from which statistical information simply cannot be discerned.[226]

2. *Committee Reporting Requirements*

Consider next the provisions involving broader reporting to congressional committees. The standards concerning each area of FISA's use largely track those in the original statute, requiring the Attorney General to "fully inform" the intelligence committees concerning use of the authorities on a semiannual basis.[227] The reporting requirements in the three NSL statutes each vary slightly, but all contain the basic "fully inform" standard. The provision concerning production of records of a wire or electronic communication service initially required the Director of the FBI to "fully inform" the intelligence committees of requests made;[228] the requirement was amended in 1993 to include the judiciary committees.[229] In the provisions governing acquisition of records from financial institutions, Congress required the Attorney General to report, on a semiannual basis, only to the intelligence committees.[230] Finally, in the provisions governing acquisition of the identity of financial institutions and identifying information from a credit reporting agency, Congress required reporting by the Attorney General to the intelligence committee and the banking committees.[231] It is not possible for an outside observer to judge the effectiveness of any of these "fully inform" requirements, although it

1:02CV2077 (executed Jan. 24, 2003) (explaining reasons for refusing to disclose "the frequency or manner of use of specific techniques authorized under FISA"), *available at* http://www.fas.org/irp/agency/?doj/?fisa/baker.pdf (last visited Mar. 30, 2005).

226. Transactional Records NSLs Since 10/26/2001 (Jan. 22, 2003), *available at* http://?www.aclu.org/?patriot?_?foia/??FOIA/??NSLlists.pdf (last visited Mar. 30, 2005).

227. *See* 50 U.S.C. § 1826 (2000) (physical searches); *id.* § 1846(a) (pen registers and trap-and-trace devices); 50 U.S.C. § 1862 (Supp. I 2001) (tangible things).

228. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867-68 (adding 18 U.S.C. § 2709 (e)).

229. *See* Act of Nov. 17, 1993 to amend title 18, U.S.C., FBI Access to Telephone Subscriber Information, Pub. L. No. 103-142, § 2, 107 Stat. 1491, 1492 (codified at 18 U.S.C. § 2709(e) (2000)).

230. *See* 12 U.S.C. § 3414(a)(5)(C) (West 2000 & Supp. 2004).

231. *See* 15 U.S.C. § 1681u(h) (West 2000 & Supp. 2004).

can safely be said that members of Congress have not always been satisfied with the Justice Department's interpretation of its obligations.[232]

In short, as the foreign intelligence surveillance framework evolved, Congress added a patchwork of public and congressional reporting requirements. Congress first began to consider a more systematic approach to reporting requirements after passage of the Patriot Act. The reporting requirements ultimately adopted along with the lone wolf amendment reflected one approach among many proposed in both houses of Congress. The provisions were first introduced by Senator Feingold as an amendment to Senate Bill 113, the lone wolf bill considered by the Senate in May 2003.[233] The amendment would have required annual reports to the intelligence and judiciary committees setting forth "the aggregate number of non-United States persons targeted for orders issued under [FISA], including a break-down of those targeted for . . ." electronic surveillance, physical searches, pen/trap coverage or compelled production of tangible things.[234]

The amendment also would have required reporting of the number of "lone wolves" covered by FISA—that is, the number of individuals determined "to have acted wholly alone in the activities covered by such order."[235] Finally, the amendment would have required information concerning the number of times the Attorney General authorized use of FISA-derived information in a criminal proceeding, and would have required disclosure "in a manner consistent with the national security of the United States" of any portions of applications and orders that include "significant construction or interpretation" of FISA.[236]

Although the Senate accepted the reporting requirement amendment without significant debate and Senate Bill 113, as amended, passed in May 2003, there was no further action on the lone wolf amendment or the accompanying reporting requirements until they were included in the Senate intelligence reform proposal in 2004. Measures identical to those included in Senate Bill 113 passed the Senate in October 2004.[237] House intelligence reform bills contained no similar reporting requirements. The version that emerged from the conference on the competing bills did

232. *See FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures—An Interim Report by Senators Patrick Leahy, Charles Grassley, and Arlen Specter* (Feb. 2003), *reprinted in* S. REP. NO. 108-40, at 13, 23-24 (2003) (expressing disappointment with "non-responsiveness of the DOJ and FBI"); H.R. REP. NO. 108-381, at 54 (2003) (noting, with respect to requirement to "fully inform" intelligence committees concerning issuance of national security letters under Right to Financial Privacy Act, that Attorney General had limited reporting to statistical information).

233. *See* 149 CONG. REC. S5913 (daily ed. May 8, 2003).

234. *Id.*

235. *Id.*

236. *Id.*

237. *See* Intelligence Authorization Act for Fiscal Year 2005, S. 2386, 108th Cong. § 304 (2004).

contain reporting requirements with only a few changes from the Senate version.[238] In particular, the final provision required semiannual rather than annual reports, and required reporting concerning all persons targeted under FISA, not merely non-U.S. persons.[239] The final version also provided that the reporting should occur "in a manner consistent with protection of national security," rather than confining that language to the provisions compelling submission of portions of applications and opinions including significant construction of FISA's provisions.[240]

If the lone wolf reporting requirements were interpreted to require public reporting, the result would be a substantial increase in the amount of publicly available information regarding FISA. Recall that the Department of Justice has presented only aggregated statistics concerning the number of electronic surveillance and physical search orders granted, modified or denied. The lone wolf amendment reporting requirements focus on the number of persons targeted rather than the number of orders, but they clearly require a statistical breakdown rather than aggregated reporting. It seems likely, however, that the Executive will interpret the provisions to permit reporting to be confined to a classified setting, even with respect to the bare statistics. The new reporting requirements were adopted against the backdrop of an array of unenacted proposals specifically calling for public release of FISA information;[241] that fact will likely be taken to reflect Congress's implicit rejection of a public reporting requirement. Indeed, in floor debate in the Senate in 2003, Senator Kyl, the sponsor of the lone wolf amendment to which the reporting requirements were being attached, explicitly stated his understanding that the reporting requirements dealt with classified reporting.[242]

If the requirements are indeed interpreted to permit classified reporting, it is unclear what information will be provided that the intelligence committees are not already entitled to receive under the "fully inform" provisions. The requirements do bring additional structure to the Justice

238. *See* Intelligence Reform and Terrorism Prevention Act of 2004, S. 2845, 108th Cong. § 6002.

239. *See* Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3743.

240. *See id.*

241. *See, e.g.*, Surveillance Oversight Act and Disclosure Act of 2003, H.R. 2429, 108th Cong. § 601; Domestic Surveillance Oversight Act of 2003, S. 436, 108th Cong. § 601; Protecting Rights of Individuals Act, H.R. 3352, 108th Cong. § 3(c) (2003).

242. *See* 149 CONG. REC. S5905 (daily ed. May 8, 2003). Senator Kyl described the amendment as requiring:

> that the information be compiled and shared with the Senate; specifically, that the information be sent to the Intelligence Committee—it is classified information, obviously—and that the cleared people on the Judiciary Committee who are appropriate to view the information have full access so that we can evaluate whether these provisions are being used, abused, how often they are being used, how effectively, and so on.

Id.

Department's reporting obligations and thus help to ensure that the "fully inform" standard is properly met. Beyond that, the requirements only have the added benefit of compelling Judiciary Committee as well as Intelligence Committee reporting. In the next section, I develop the case for broader public reporting as well as other changes to the foreign intelligence surveillance framework.

C. *Rethinking FISA's Information Structure*

As the discussion above suggests, as the foreign intelligence surveillance framework evolved from a single investigative tool to be used in relatively narrow circumstances to encompass seven distinct authorities involving different substantive standards and procedural provisions, Congress did not systematically consider what oversight changes would be necessary to ensure an adequate balance between privacy and security and to ensure fidelity to statutory intent. In extending FISA's reach to cover lone wolf terrorists, Congress for the first time enacted a set of reporting requirements designed to take account of the foreign intelligence surveillance framework as a whole. That development is certainly a welcome one. As I argue below, however, Congress has more work to do in improving FISA's information structure.

I discussed above the fact that limited post-surveillance judicial involvement raises concerns about substantive outcomes and about legitimacy. The question is whether FISA's current information structure adequately addresses these concerns, and if not, what institutional mechanisms can do so better. I consider first the issue of legitimacy. As noted, the detailed procedure that FISA imposes on the executive branch—requiring certifications by national security officials and the Attorney General's written approval—reflected Congress's belief that such a measure would serve a privacy protective function, and thus enhance the legitimacy of the FISA process. Of course, the procedures are far more elaborate in the context of the main (electronic surveillance and physical search) foreign intelligence surveillance authorities than in the context of the "lesser" (pen register and trap-and-trace device, tangible things and NSL) authorities. Even with respect to the main FISA authorities, however, if the executive branch's or the FISC's interpretation of the various statutory requirements is never publicly revealed, the legitimacy of the FISA process depends entirely on the public's willingness to trust an entirely secret process.

The requirements to "fully inform" the intelligence committees concerning implementation of FISA, or the more specific recent requirements to provide statistical and other information to the intelligence and judiciary committees, cannot alone address the legitimacy concerns, for they do nothing to clarify for the public the extent of the statute's use or abuse. As for the public reporting of statistics on FISA's use, the neglect of the statistical reporting requirement since 1978 makes it unlikely that the

current level of statistical reporting can overcome any legitimacy problems, particularly now that the number of orders granted under FISA's electronic surveillance and physical search authorities exceeds the number of electronic surveillance orders granted under Title III.[243]

Assessing whether FISA's current information structure addresses concerns about substantive outcomes proves complex, in part because of the difficulty in assessing the effectiveness of the requirements to "fully inform" the congressional intelligence committees concerning FISA's use. Two general points can be made, however. First, in enacting FISA in 1978, Congress recognized the importance of the public statistical reporting to fulfillment of Congress's oversight functions.[244] There is a strong theoretical justification for Congress's reliance on public as well as inter-branch reporting. From an institutional design perspective, the (public) statistical reporting requirement and (classified) requirement to "fully inform" the intelligence committees can be viewed as complementary: The first reflects what political scientists and administrative law scholars might refer to as a "fire-alarm" model of oversight, where Congress adopts mechanisms that facilitate individual citizens' and interest groups' ability to bring problems to Congress's attention, while the second reflects a "police-patrol" model of oversight, where Congress itself actively gathers information.[245]

Second, the evidence on whether the "fully inform" requirements have allowed Congress to fulfill its oversight function in such a way as to make appropriate changes to FISA's structure is somewhat discouraging. In particular, it could be argued that Congress has on at least some occasions unnecessarily expanded statutory authorities for foreign intelligence surveillance, where the problems Congress sought to address stemmed from erroneous interpretations of FISA by the executive branch. Two ex-

243. *Compare* Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, U.S. Dep't of Justice, to L. Ralph Mecham, Director, Administrative Office of United States Courts (Apr. 30, 2004) (noting approval of 1724 applications for electronic surveillance and physical searches under FISA during calendar year 2003), *at* http://?www.usdoj.gov/?oipr/?readingroom/?2003fisaltr.pdf (last visited Jan. 29, 2005), *with* Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (Apr. 2004) (noting approval of 1442 state and federal wiretap orders under Title III during calendar year 2003), *available at* http://?www.?uscourts.?gov/?wiretap03/?2003WireTap.pdf (last visited Feb. 20, 2005).

244. For a discussion of the reporting requirements contemplated by Congress, see *supra* note 214. and accompanying text (emphasizing heightened need for oversight in foreign intelligence context). *See also* S. REP. NO. 95-604, pt. 1, at 60, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3961 (noting that statistical reporting "should present a quantitative indication of the extent to which surveillance under this chapter [is] used" and that "[t]he statistics reported pursuant to this section will provide a basis for further inquiry by appropriate oversight committees of the Congress").

245. *See, e.g.*, Mathew D. McCubbins & Thomas Schwartz, *Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms*, 28 AM. J. POL. SCI. 165, 166 (1984).

amples illustrate the point, although again the secrecy surrounding the FISA process makes it difficult to fully evaluate either.

First, it could be argued that the lone wolf amendment itself was an unnecessary legislative response to purely bureaucratic problems. FBI agents abandoned their efforts to obtain a FISA order concerning Moussaoui after attorneys at FBI Headquarters concluded that the evidence linking Moussaoui to a "foreign power" was insufficient. Both the 9/11 Commission Report and an earlier congressional inquiry into intelligence failures leading up to the 9/11 attacks, however, noted that the Minneapolis agents gathering information for the FISA application, apparently misled by Headquarters attorneys, proceeded upon the erroneous premise that only a "recognized" terrorist group—that is, one on the State Department's official list of foreign terrorist organizations[246]—could qualify as a foreign power for purposes of FISA.[247]

FISA does not require that an organization be on the State Department's list of designated terrorist organizations to trigger FISA coverage; the statute requires only that the group be one engaged in international terrorism, or activities in preparation therefor.[248] Some evidence apparently suggested a link between Moussaoui and Chechen rebels,[249] but agents' belief that such a link would be insufficient for purposes of the statute (because the Chechen rebels did not constitute a "recognized" terrorist group) prompted other efforts, ultimately futile, to establish a link between the Chechen rebels and Al Qaeda.[250]

Even without this mistake concerning the need to link Moussaoui to a designated terrorist group, it is not clear whether the Moussaoui application would have gone forward. But it is also not clear whether the lone wolf amendment's loosening of the "agent of a foreign power" requirement was an appropriate congressional response. In particular, reviews of the FISA process from within the executive branch, Congress and elsewhere have suggested that the gatekeeper to the FISC, the Justice Department's Office of Intelligence Policy and Review (OIPR), has applied a too-

246. *See, e.g.*, Office of Counterterrorism, U.S. Dep't of State, Fact Sheet: Foreign Terrorist Organizations (Dec. 29, 2004) (providing current list of designated foreign terror organizations), *at* http://www.state.gov?/s?/ct?/rls?/fs/?2004/?37191.htm (last visited Jan. 29, 2005).

247. *See* 9/11 COMMISSION REPORT, *supra* note 3, at 274; JOINT INQUIRY, *supra* note 1, at 321; *see also* S. REP. NO. 108-40, at 11 (2000) (additional views of Sens. Leahy and Feingold) (arguing that "the FBI had all the evidence it needed to procure [a FISA warrant] had they only understood the proper legal standard"); *Interim Report on FBI Oversight in the 1978 Congress by the Senate Judiciary Committee: FISA Implementation Failures, reprinted in* S. REP. NO. 108-40, at 34 (2000) [hereinafter *Interim Report*].

248. 50 U.S.C. § 1801(b)(2)(C) (2000).

249. *See* 9/11 COMMISSION REPORT, *supra* note 3, at 274; JOINT INQUIRY, *supra* note 1, at 321.

250. *See* 9/11 COMMISSION REPORT, *supra* note 3, at 274; JOINT INQUIRY, *supra* note 1, at 321.

stringent standard of probable cause, leading to anticipatory rejection of FISA requests by FBI Headquarters attorneys.

Prior to implementation of the Patriot Act's changes to FISA, the FISC had only once denied a FISA request, and then at the Executive's urging—when the Reagan Administration sought clarification that the FISC lacked jurisdiction under the original FISA to grant orders authorizing physical searches.[251] That statistic is a source of pride for OIPR, which argues that its well-scrubbed applications are closely scrutinized by FISC judges, who often return applications to OIPR for further development and modification rather than denying requests.[252] As observers have suggested, however, it is also plausible that OIPR's perfect record results from the FBI's or OIPR's application of a too-high standard of probable cause.[253] Indeed, at oversight hearings on the FISA process conducted in 2002, FBI attorneys responsible for evaluating FISA applications expressed uncertainty about how the Supreme Court had construed the probable cause requirement in the criminal context.[254] Other episodes in FISA's history, most notably the Wen Ho Lee matter, have raised similar concerns about the Executive's handling of FISA applications.[255]

I do not intend to suggest that the Moussaoui FISA application should have been presented to the FISC and granted; without more public information about precisely what investigators knew at the time, it is difficult to say whether probable cause existed that Moussaoui was an agent of a foreign power. The uncertainty on this point simply reinforces the observation that it is difficult to distinguish situations in which foreign intelligence investigative authorities are inadequate from situations in which those authorities are being misunderstood or misapplied.

Indeed, a case can be made that even the most important of the Patriot Act's FISA changes—from requiring a national security official's certification that "the purpose" of FISA coverage is to obtain foreign intelligence to requiring certification that "a significant purpose" of FISA coverage is to obtain foreign intelligence information—reflected a legislative response to an erroneous interpretation of FISA. If that interpreta-

251. *See supra* note 135 and accompanying text.

252. *See, e.g.*, Wittes, *supra* note 83.

253. *See* BELLOWS REPORT, *supra* note 179, at 493 ("While there is something almost unseemly in the use of such a remarkable track record as proof of error, rather than proof of excellence, it is nevertheless true that this record suggests the use of ['probable clause plus'], an insistence on a bit more than the law requires."). For other assessments reaching similar conclusions, see, for example, NATIONAL COMMISSION ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM 11 (2000) ("[T]he statute requires only probable cause to believe that someone who is not a citizen or legal permanent resident of the United States is a member of an international terrorist organization. In practice, however, OIPR requires evidence of wrongdoing or specific knowledge of the group's terrorist intentions . . . ."), *at* http://www.gpo.gov/nct/nct5.pdf (last visited Jan. 29, 2005).

254. *See Interim Report*, *supra* note 247, at 38.

255. *See* BELLOWS REPORT, *supra* note 179, at 493.

tion emanated from the FISC rather than the executive branch, then legislation was indeed necessary to correct it. But the particular response Congress chose in enacting the USA Patriot Act has arguably entrenched a broader power than necessary to correct the misinterpretation.

As noted, several courts applying pre-FISA case law assumed or held that FISA coverage could be sought and granted only where the "primary purpose" of the investigation was to gather foreign intelligence information.[256] The pre-FISA case that first applied the "primary purpose" test assessed when foreign intelligence gathering was no longer the investigation's "primary" purpose by measuring the level of involvement of criminal investigators and prosecutors in the investigation.[257] Fears that the FISC would deny FISA coverage or its renewal in investigations in which criminal investigators were too heavily involved led to the development of a "wall" between counterintelligence and criminal investigators, which was formalized in the 1995 Attorney General Guidelines.[258] The Patriot Act's "significant purpose" change was in large measure designed to remove that wall. In the absence of more public information, it is difficult to assess the extent to which the 1995 Guidelines were driven by the FISC's interpretation of the "the purpose" language (or a Fourth Amendment gloss on that language), or by the Justice Department's desire to avoid stepping anywhere near the statutory or constitutional line. In either case, however, it is not clear that the pre-Patriot Act language required the strict counterintelligence/?criminal separation that the 1995 Guidelines imposed. In other words, whether the underlying interpretation was that of the FISC or that of the Justice Department, it could well have been erroneous.

The difficulty with the particular solution Congress adopted in response to the too-strict separation of counterintelligence and criminal authorities is that it may have entrenched a broader investigative power than necessary to address the underlying problem. One could read the "significant purpose" language, against the backdrop of pre-FISA case law and the 1995 Attorney General Guidelines, as having been designed to insure that *involvement* of criminal investigators should not preclude FISA coverage. But the "significant purpose" change has been interpreted to permit not merely *involvement* of criminal investigators, but *direction and control* of FISA investigations by criminal investigators.[259]

We cannot, of course, conclude that weaknesses in the foreign intelligence surveillance framework's information structure are solely or even significantly responsible for these questionable legislative changes. Indeed, one could argue that the facts underlying the controversy over the

256. *See supra* notes 180-88 and accompanying text.

257. *See supra* notes 185-88 and accompanying text.

258. *See supra* notes 178-79 and accompanying text.

259. *See In re* Sealed Case, 310 F.3d 717, 728-36 (Foreign Intel. Surv. Ct. Rev. 2002).

1995 Guidelines can only be recounted here because of the robust reporting on the use of the FISA process that accompanied the Justice Department's extensive investigation of the Wen Ho Lee matter[260]—that, in other words, episodic but detailed reporting on FISA's implementation triggered Congress's conclusion that implementation of FISA was inconsistent with its intent. But just as we cannot definitively link the need for legislative changes to FISA to a failure to provide mechanisms that reveal questionable interpretations of the statute before those interpretations become entrenched, we cannot assume that the sort of episodic public reporting that might result from particular investigative failures will adequately measure the Executive's and the FISC's fidelity to the statutory structure.

As this discussion suggests, FISA's current information structure does not adequately address concerns about substantive outcomes and legitimacy. In light of the expansion of the foreign intelligence surveillance framework from a single narrow electronic surveillance authority to encompass a range of investigative authorities, Congress's recognition of the importance of public reporting, and institutional design considerations, there are powerful arguments for broader public reporting than currently occurs. The lack of any statistical reporting makes public awareness of the extent of foreign intelligence surveillance impossible. No matter how thoroughly Congress examines FISA activities under the "fully inform" standard, in the absence of even the most basic public reporting the public is likely to remain deeply skeptical of the need for foreign intelligence investigative authorities and suspicious of how those authorities are implemented. The difficulty, of course, lies in identifying the maximum level of public reporting consistent with national security.

As a starting point, Congress could alter the newly enacted reporting requirements (i.e., those accompanying the lone wolf amendment) to require public reporting. As discussed earlier, the provisions require reporting of a statistical breakdown of the number of persons targeted under provisions authorizing electronic surveillance, physical searches, use of pen registers and trap-and-trace devices and compelled production of tangible things. (Regardless of whether Congress requires broader public reporting, it should expand this requirement to encompass a statistical breakdown of the executive branch's use of NSL authorities).

In addition, the provisions require disclosures concerning the number of times the Attorney General has authorized the use of FISA-derived information in a criminal proceeding, as well as the release of any portions of applications and orders including significant construction or interpretation of FISA. The Justice Department would likely oppose any expansion of its public reporting obligations. In resisting proposals to expand those obligations in the past, the Justice Department has consistently argued that any public release of statistical information on the use of specific in-

260. *See* BELLOWS REPORT, *supra* note 179, at 552-688.

vestigative techniques "would harm our national security."[261] Such concerns certainly deserve the most serious consideration, and it is difficult for an outside observer to evaluate them fully.

Some of the Department's arguments—for example, that disaggregating the number of U.S. persons and non-U.S. persons subject to FISA surveillance or searches would signal to foreign powers the degree to which reliance on U.S. persons in clandestine intelligence activities would shield them from scrutiny[262]—seem compelling. Others seem more questionable. For example, the Justice Department has consistently refused to release a statistical breakdown of how it uses each of the FISA authorities. But aggregated statistics on two foreign intelligence authorities (electronic surveillance and physical searches) are of course already publicly reported. Because it appears that physical searches under FISA occur relatively infrequently, statistics on electronic surveillance are already roughly known or can be extrapolated from past reporting. Given the knowledge that already exists concerning the extent of the executive branch's use of electronic surveillance techniques to capture the contents of communications, it is difficult to see how reporting on the use of related devices (i.e., pen registers and trap-and-trace devices) would provide any greater strategic advantage or have a stronger deterrent effect on the use of particular communications technologies than current reporting on electronic surveillance provides or has.

Similarly, with respect to those authorities concerning compelled production of records or other items—FISA's tangible things provision and the separate national security letter authorities—the Justice Department's position seems premised upon the dubious proposition that foreign powers or their agents could or would avoid dealing with covered third party institutions if the precise extent of the Executive's use of the intelligence gathering authorities became known.

Just as it has opposed additional statistical reporting, the Justice Department has claimed that an obligation to release information concerning significant constructions or interpretations of FISA is inappropriate. It is worth noting, however, that broader public reporting on significant legal questions is consistent with the early history of FISA's implementation. As noted earlier, in the first five years of FISA's implementation, Congress released a series of statutorily required reports on FISA's implementation. I have already alluded to one early controversy surrounding interpretation of FISA—that concerning the jurisdiction of the FISC to issue orders authorizing physical searches under the original FISA statute. The congres-

261. Declaration of James A. Baker, Counsel for Intelligence Policy, at 6-7, American Civil Liberties Union v. U.S. Dep't of Justice, Civ. Action No. 1:02CV2077 (executed Jan. 24, 2003) (explaining reasons for refusing to disclose "the frequency or manner of use of specific techniques authorized under FISA"), *available at* http://www.fas.org/irp/agency/doj/fisa/baker.pdf; 149 CONG. REC. S5923-24 (daily ed. May 8, 2003).

262. *See* 149 CONG. REC. S5923 (daily ed. May 8, 2003).

sional reports provide a great deal of context for that dispute, and include Justice Department and FISC legal memoranda on the subject. The release of the briefs and opinions concerning the Justice Department's interpretation of the Patriot Act similarly illustrate the potential for public scrutiny of rulings on pure issues of law.

Again, I do not intend to minimize the national security concerns that the Justice Department has raised concerning broader reporting. My point is simply that Congress should consider these objections with a healthier degree of skepticism than it has in the past. Even if Congress did require the executive branch to report publicly what the recently enacted provisions seem to permit it to report in a classified setting, the executive branch could of course claim that national security considerations precluded the release of the information. A broader public reporting requirement would nevertheless have the effect of shifting the baseline presumption from one of withholding information to one of disclosing it. At present, in the absence of any specific requirement for public reporting of statistical information on use of FISA and NSL authorities, it is all too easy for the Executive to deny access to such information in the name of national security.

Whether or not Congress (or the executive branch) concludes that the sort of specific statistical reporting described above can be publicly released, Congress should consider reinstating and extending the requirement that the Intelligence Committees report to the Senate and the House concerning implementation of FISA. As noted, the congressional reports from the early years of FISA's implementation provided a great deal of context for one dispute going on at that time—concerning whether the FISC had authority to grant physical search orders. It seems unlikely that there would otherwise have been any public awareness of the dispute. Reinstating the requirement for Intelligence Committee reports would encourage congressional and executive accommodation, on an ad hoc basis, concerning what information is appropriate for public release. Quite apart from the substantive impact that a broader public release of information might have on the foreign intelligence surveillance framework, this sort of committee reporting would have substantial benefits in terms of legitimacy. The early committee reports tend to illustrate the executive branch's narrow and careful use of FISA.

Finally, FISA's information structure would be significantly improved with the declassification of more information concerning use of the various statutory authorities, even if many years after the fact. It is difficult to believe that national security considerations require the continued classification and nondisclosure of all aspects of all applications and orders considered and granted since FISA's enactment in 1978. An existing provision concerning the use of information obtained from a physical search under FISA offers one possible model. The statute requires that:

> [w]here a physical search . . . involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search . . . and shall identify any property of such person seized, altered, or reproduced during such search.[263]

This provision is quite narrow, in that it applies only where a *residence* of a U.S. person is searched, not where any personal property of a U.S. person is searched. Congress could expand the provision to cover personal property and insert parallel provisions with respect to other foreign intelligence surveillance authorities. Again, the default presumption under the provision is that notice will not occur. Congress could shift the default presumption to one of disclosure by, for example, providing that the Attorney General shall provide the requisite notice not later than five years after the investigative activity occurs unless he or she concludes that there is a national security interest in maintaining the secrecy of the search.

The proposals offered above have focused solely on how to achieve the maximum degree of public reporting consistent with national security. It is worth mentioning one more institutional mechanism proposed to Congress on various occasions in the past that would have substantial benefits for the FISA process: the use of security-cleared counsel to oppose FISA applications, at least in those cases involving U.S. persons.[264]

Even the FISCR, at oral argument of the Government's appeal challenging the FISC's en banc interpretation of the Patriot Act's "significant purpose" amendment, commented on the awkwardness of the non-adversarial nature of the proceedings before it.[265] In terms of legitimacy, the benefits of having security-cleared opposing counsel argue before the FISC are obvious: doing so would ensure that, despite the secrecy of the FISA process, concerns about FISA's application in particular factual contexts were fully aired. Moreover, use of opposing counsel would relieve

---

263. 50 U.S.C. § 1825(b).

264. *See, e.g., The USA PATRIOT Act in Practice: Shedding Light on the FISA Process, Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. 96 (2002) (prepared statement of Kenneth C. Bass III) [hereinafter *Bass Statement*].

265. *See* Hearing on Docket No. 02-001, at 100 (Foreign Intel. Surv. Ct. Rev.) (Sep. 2, 2002) (Guy, J.) ("This is a strange proceeding because it is not adversarial. It is ex parte. And if one were to just read the transcript of this hearing today one might think that the adversary, if there was one, is what the insiders refer to as the FISC . . . ."), *available at* http://www.fas.org/?irp/?agency/?doj/?fisa/?hrng090902.htm (last visited Aug. 11, 2004); *see also id.* at 37 (Silberman, J.) (reminding those present that proceeding had no adversary); *id.* at 67-68 (Silberman, J.) (reiterating that hearing was *ex parte* proceeding).

any pressure on both OIPR and the FISC itself to act as "devil's advocate" by narrowly interpreting the statute.[266]

As this discussion suggests, in enacting FISA in 1978, Congress recognized the limits on post-surveillance judicial review, as well as the consequences of those limits for legitimacy of the FISA process and for substantive outcomes, both in individual cases and systemically. Congress thus placed privacy safeguards and information-generating mechanisms outside of the judiciary. But FISA's information structure has not kept pace with other statutory changes. I have argued here for various additional mechanisms to expand FISA's information structure. Again, an outside observer cannot have a sufficiently broad perspective on the foreign intelligence surveillance process to fully consider the implications of these proposals. Although the mechanisms proposed here seem feasible and appropriate in light of what can be gleaned from public information about the foreign intelligence surveillance process, other factors may counsel in favor of narrower or different solutions. At a minimum, however, Congress must confront the executive branch's national security objections to greater public reporting with a healthier degree of skepticism than it has in the past.

V. CONCLUSION

The approach of the December 31, 2005, sunset date for many of the post-9/11 surveillance law changes provides Congress with an opportunity to rethink the foreign intelligence surveillance framework. When passed in 1978, FISA reflected a careful accommodation of security and privacy interests. Since that time, Congress has made episodic, piecemeal changes, to the point where the executive branch can engage in foreign intelligence surveillance activities in a far broader range of circumstances than in 1978. Courts play a necessarily diminished role in the foreign intelligence surveillance process.

The FISC evaluates executive branch applications for surveillance, but, in light of the secrecy surrounding the process, the FISC's activities do not result in any public articulation of legal norms. Although the careful institutional design choices Congress made in 1978 to some degree responded to this problem—by using public and congressional reporting as a privacy safeguard and as a source of information on statutory implementation—the institutional design has not kept pace with the congressional expansion of foreign intelligence surveillance. No matter how Congress resolves the various substantive issues likely to arise in the Patriot Act re-

266. *See Bass Statement, supra* note 264, at 96. Mr. Bass stated the following:

> When there is no counsel on "the other side," the court finds itself in an uncomfortable position of being critic as well as judge. I believe the May 17, 2002 amended decision and order of the FISC reflects the built-up tension in that Court's role, a tension exacerbated by the total absence of an adversarial process.

Id.

newal debate—including the "significant purpose" language and the lone wolf provision—Congress should expand FISA's information structure to properly correspond with its expansion of foreign intelligence surveillance powers.