

Programmatic Surveillance and FISA: Of Needles in Haystacks

William C. Banks*

Beginning in 1978, the Foreign Intelligence Surveillance Act¹ (FISA) authorized the means for electronic collection of foreign intelligence that served the nation well for many years. The basic idea was simple. Government may conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime if it could demonstrate to a special Article III court that it had a different kind of probable cause: reason to believe that targets of surveillance are acting on behalf of foreign powers.² Over time, FISA was amended several times to extend its procedures to conduct physical searches,³ monitor suspected lone-wolf terrorists,⁴ and accommodate evolving threats.⁵

Over the last decade, critics have argued that the patchwork-like architecture of FISA has become too rigid, complicated, and unforgiving to enable effective intelligence responses to crises.⁶ The computerization of communications that has so enriched our capabilities has also facilitated

* Director, Institute for National Security and Counterterrorism; Board of Advisors Distinguished Professor, Syracuse University College of Law; Professor of Public Administration, Maxwell School of Citizenship & Public Affairs, Syracuse University. The author thanks Spike Bowman, Stephen Dycus, Alexander Joel, Peter Raven-Hansen, Kim Taipale, and the participants in the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology, Feb. 4–6, 2010, for comments on a draft of this article. The author also thanks Andrea Masselli, Syracuse University College of Law, J.D. 2010, for excellent research assistance.

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

2. *Id.* § 105(a) (codified at 50 U.S.C. § 1805(a)).

3. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807, §§ 301–309, 108 Stat. 3423, 3443–53 (codified as amended at 50 U.S.C. §§ 1821–1829).

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

5. See FISA § 105(b)(2)(B) (requiring an order approving electronic surveillance to direct, at the applicant's request, a communication or other common carrier to assist an applicant in accomplishing the surveillance in a manner to protect its secrecy and minimize interference with the carrier's services); *Id.* § 105(b)(1)(B) (requiring an application to identify the facilities where surveillance will be sought "if known").

6. See, e.g., Richard A. Posner, Op-Ed., *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16 (arguing that FISA is "dangerously obsolete"); K.A. Taipale & James Jay Carafano, Op-Ed., *Fixing Surveillance*, WASH. TIMES, Jan. 25, 2006, at A15. Judge Posner has claimed that FISA "remains usable for regulating the monitoring of communications of known terrorists, but it is useless for finding out who is a terrorist." Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 252 (2008).

stealth and evasion by those seeking to avoid detection.⁷ Would-be targets of surveillance are communicating in ways that stress or evade the FISA system.⁸ Because of the pervasiveness of U.S. telecom switching technology, collection *inside* the United States is now often the best or only way to acquire even foreign-to-foreign communications that were originally left unregulated by FISA.⁹ Meanwhile, powerful computers and data-mining techniques now permit intelligence officials to select potential surveillance targets from electronic databases of previously unimaginable size.¹⁰ The wholesale quality of this expansive computer collection and data mining is incompatible with the retail scope of the original FISA process.¹¹ Instead of building toward an individual FISA application by developing leads on individuals with some connection to an international terrorist organization, for example, officials now develop algorithms that search thousands or even millions of collected e-mail messages and telephone calls for indications of suspicious activities.¹²

At the same time, more Americans than ever are engaged in international communications, and there is far greater intelligence interest in communications to and from Americans.¹³ Both circumstances increase the likelihood that the government will be intercepting communications of innocent Americans, raising as many questions about the adequacy of FISA safeguards as they do about the adaptability of FISA architecture. This tension forms the context for a series of post-9/11 developments, culminating in the FISA Amendments Act of 2008 (FAA).¹⁴

7. See William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1275–76 (2007) (observing that, in the world of technological surveillance, evasion and logistical difficulties force the government to continually play “catch-up”).

8. *Id.*

9. See David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come* (noting that after FISA’s enactment, the need to “conduct surveillance of international communications on wires *inside* the United States” developed, in part because of “the use, location, or accessibility of fiber optic cables”), in *LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM* 217, 226 (Benjamin Wittes, ed., 2009).

10. See, e.g., JAMES BAMFORD, *THE SHADOW FACTORY: THE ULTRA SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA* 12–14 (2008) (describing the vast data-collection capabilities of the NSA).

11. See Josh Meyer & Joseph Menn, *U.S. Spying is Much Wider, Some Suspect*, L.A. TIMES, Dec. 25, 2005, at A1 (investigating concerns that the NSA’s wholesale collection of communication data exceeded FISA and threatened Americans’ privacy).

12. See Shane Harris, *FISA’s Failings*, NAT’L J., Apr. 8, 2006, at 59, 59 (“[T]he NSA’s warrantless eavesdropping program also involves looking for suspicious patterns in a sea of communications.”).

13. See Leslie Cauley, *NSA Has Massive Database of Americans’ Phone Calls*, USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (“[T]he National Security Agency has been secretly collecting the phone call records of tens of millions of Americans [T]he spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity”).

14. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463 (to be codified in scattered sections of 50 U.S.C.).

The FAA codified a procedure to permit broad, programmatic surveillance focused on patterns of suspicious activities and not on a specific individual or the contents of their communications through changes in FISA that overcame the case-specific orientation of the original statute.¹⁵ As a result, the FAA also codifies, until December 31, 2012, potentially intrusive electronic surveillance unaccompanied by safeguards to protect personal privacy and free expression.¹⁶ The amended FISA also institutionalizes operations that are prone to inaccuracy and chronic overcollection.¹⁷ A 2008 decision by the FISA Court of Review (FISCR),¹⁸ which upheld the government's implementation of the programmatic procedures of earlier but similar temporary legislation¹⁹ by relying on procedures drawn from sources outside FISA, underscores the slapdash development and still-incomplete legal architecture that attends the broad-based programmatic orders.²⁰

From its beginnings, the overarching FISA question has been how to evaluate and weigh the basic values of security and individual liberties when intrusive electronic surveillance is used to collect foreign intelligence. Modern communications and surveillance technologies have so complicated policy discussions, however, that the values debate has drowned in a sea of misapprehension about the means to implement the policies.²¹ Meanwhile, FISA has become so complex that the law further occludes informed policy choices.²² The basic architecture of FISA should be recast.

The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the United States if the surveillance involves U.S. persons who do not have a connection to a foreign power.²³ FISA now

15. *See id.* § 702(a)–(e) (specifying the requirements for acquiring communications data and setting out targeting and minimization protocols).

16. *See id.* § 403 (indicating that the codification is to expire on December 31, 2012).

17. *See infra* notes 105–07 and accompanying text.

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

19. Protect America Act of 2007, Pub. L. No. 110-55, §§ 2–3, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805(a)–(c)).

20. *See In re Directives*, 551 F.3d at 1010 (recognizing the lack of an explicit foreign intelligence exception, but reasoning from the “special needs” cases that an exception to the warrant requirement was appropriate).

21. *See* Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 246–47 (discussing modern computer technology and its complication of the values debate shaping lawmaking in the field of electronic surveillance).

22. *See* Banks, *supra* note 7, at 1214–15 (arguing that the cumulative complexity of FISA has led to the loss of the policy compromise between enabling surveillance and using oversight mechanisms to safeguard individual privacy); Posner, *A New Surveillance Act*, *supra* note 6 (arguing that the “best, and probably the only, way” to clarify the government’s ability to conduct electronic surveillance is to “enact a new statute”).

23. *See* *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 320–22 (1972) (holding that a warrant is required to conduct domestic surveillance, but limiting that holding to purely domestic threats to national security).

permits such electronic surveillance as the inevitable byproduct of surveillance of unprotected targets, but the Act does little to insulate U.S. persons from the effects of the surveillance. (It is not clear whether the Fourth Amendment Warrant Clause applies to such surveillance when a U.S. person is connected to a foreign power, or when the surveillance of U.S. persons occurs wholly outside the United States. The reasonableness component of the Fourth Amendment does apply in these instances.)²⁴ Historically, our laws have rejected granting discretion for government to undertake intrusive surveillance of individuals without some showing of suspicious activities.²⁵ If the combination of terrorism threats and computerization demands a more nimble capacity to conduct suspicionless electronic surveillance to combat terrorism, the discretion that is necessarily part of that system should be more carefully controlled, either at the point of collection or when the information is maintained or used by the government. Absent such controls, FISA as amended now threatens longstanding Fourth Amendment principles. Apart from its potential constitutional shortcomings, the programmatic surveillance that the FAA permits should be repaired to improve its efficacy. Making the program more efficacious will help make it lawful.

Even before programmatic surveillance was stitched onto FISA, the Act labored under continuing controversies over lowering the wall that separated intelligence from law enforcement investigations²⁶ and the inconsistency of requiring probable cause of foreign agency for targets while permitting surveillance of lone wolves.²⁷ Programmatic surveillance adds considerably to complexity, has already produced implementation problems, and casts doubt on the lawfulness and efficacy of FISA's techniques.

In Part I and Part II of this Article, I will review the FISA model for authorizing surveillance for foreign intelligence purposes and how the combination of evolving technologies and emerging terrorism threats caused FISA to become too unwieldy and inflexible to accommodate the needs for speedy and agile surveillance. In Part III, I will describe how the Bush Administration's Terrorist Surveillance Program (TSP) led to the temporary Protect America Act (PAA), and then to the FAA and the codification of programmatic surveillance. After reviewing a FISCR decision upholding the temporary version of programmatic FISA procedures and taking note of

24. A lower federal court has upheld an exception to the Fourth Amendment Warrant Clause for searches conducted for foreign intelligence purposes outside the United States that involve U.S. persons acting as foreign agents, although in other respects a search still must be reasonable. *See United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000) (adopting a foreign intelligence exception to the warrant requirement for searches targeting foreign powers or their agents conducted abroad). The Supreme Court has not ruled on either set of questions.

25. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (holding that invasion of a constitutionally protected area without a warrant is presumptively unreasonable).

26. Banks, *supra* note 7, at 1241–54.

27. *See, e.g., id.* at 1271–74 (discussing the debate surrounding the adoption of the 2004 Amendment that expanded FISA's reach to unaffiliated persons).

some implementation problems with the FAA in Part IV, in Part V I will suggest some benchmarks for rebuilding FISA from the ground up.

The programmatic features are likely here to stay. For legal and policy reasons, these features should be improved. The thirty-year linchpin of FISA targeting—the location, identity, or both, of the target—should be abandoned where it is not known. Instead, applications for programmatic surveillance under FISA should be based on showing that the proposed electronic surveillance is material to an ongoing investigation of international terrorism or clandestine intelligence activities, that alternative investigative techniques are not capable of collecting the information, and that it is likely that conducting the surveillance will provide the information sought.

A second set of reforms should focus on the retention and dissemination of what is collected. Congress should create a standardized system for authorized use of collected information across the Executive Branch. Building on an authorized-use platform, the Department of Justice and the Office of the Director of National Intelligence should develop guidelines that account specifically for the unique dynamics of protecting personal information about U.S. persons that is collected, even inadvertently, in programmatic collection. In addition, where programmatic surveillance is requested, the FISA Court (FISC) should, before and periodically during implementation, review and approve minimization procedures that are tailored to assess the efficacy and impact on privacy, free expression, and security of the mega-collection and data-mining techniques employed. In the aggregate, a combination of administrative safeguards and judicial and congressional oversight that is more robust than what is now required should be built into the programmatic surveillance portion of FISA.

I. The Original Architecture

Until the FAA, FISA governed the electronic surveillance and physical searches only of persons in the United States and only for the purpose of collecting foreign intelligence.²⁸ (FISA did not apply to surveillance or searches conducted outside the United States or to foreign-to-foreign telephone communications intercepted within the United States.)²⁹ “Probable cause” required that a target of the surveillance be a “foreign power,”³⁰ an “agent of a foreign power,”³¹ or, since 2004, a “lone wolf” terrorism

28. See FISA Amendments Act of 2008, Pub. L. No. 110-261, §§ 701–708, 122 Stat. 2436, 2438–59 (to be codified at 50 U.S.C. §§ 1881–1881g) (relating to “Persons Outside the United States”).

29. See Banks, *supra* note 7, at 1230 (explaining that in 2008 the definition of *electronic surveillance* excluded surveillance taking place abroad).

30. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1783, 1790 (codified at 50 U.S.C. § 1805(a)(3)(A) (2006)).

31. *Id.*

suspect.³² Applications to the FISC for approval of a search or surveillance had to specify “facilities” where the surveillance would be directed³³ and procedures to “minimize” the acquisition, retention, and dissemination of information not relevant to an investigation.³⁴ A special court, the FISC, which meets in secret, was created to hear requests for orders to conduct the surveillance.³⁵

For a long time the process worked well as a mechanism to regulate surveillance of known intelligence targets.³⁶ The FISA process and its eventual orders have always been limited, however. FISA was concerned with acquisition, not with the uses government might have for what is collected. FISA also assumed that officials know where the target is and what facilities the target will use for his communications.³⁷ Knowing this much enabled the government to demonstrate the required probable cause to believe that the target was an agent of a foreign power or a lone wolf.³⁸ FISA did *not* authorize intelligence collection for the purpose of *identifying* the targets of surveillance, or of collecting aggregate communications traffic and then identifying the surveillance target.³⁹ In other words, FISA envisioned case-specific surveillance, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications.⁴⁰ FISA was also based on the recognition that persons lawfully *in* the United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.⁴¹

Although the volume of FISA applications increased gradually through the 1990s,⁴² after 9/11 the pace of electronic intelligence collection quickened, and Bush Administration officials argued that traditional FISA procedures interfere with necessary “speed and agility.”⁴³ As the pre-9/11

32. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 101(b)(1), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2006)) (defining *agent of a foreign power* as “any person other than a United States person, who engages in international terrorism or activities in preparation thereof”).

33. FISA § 105(b)(1)(B).

34. FISA § 101(h); *see also* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807, § 301(4), 108 Stat. 3423, 3443–44 (codified at 50 U.S.C. § 1821(4) (2006)) (amending FISA to include a new definition for “minimization procedures”).

35. FISA § 103.

36. *See* Banks, *supra* note 7, at 1233–40 (detailing the operation of FISA between 1978 and the early 1990s).

37. Banks, *supra* note 7, at 1231–32.

38. *Id.* at 1260.

39. *Id.* at 1276.

40. *Id.*

41. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1783, 1790 (codified at 50 U.S.C. § 1805(a)(3)(A) (2006)).

42. Banks, *supra* note 7, at 1233–34.

43. *Administration Defends NSA Eavesdropping to Congress*, CNN.COM, Dec. 23, 2005, <http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html>.

FISA applications doubled to more than 2,000 a few years later,⁴⁴ the Director of National Intelligence (DNI) complained that more than “200 man hours” are required to prepare an application “for one [phone] number.”⁴⁵ The system was, it seemed, grinding along, but it was carrying a lot of weight.

II. Technological Stresses on FISA

Meanwhile, with the revolution in digital communications, the idea of a geographic border has become an increasingly less viable marker for legal authorities and their limits. Using the Internet, packets of data that constitute messages travel in disparate ways through networks, many of which come through or end up in the United States.⁴⁶ Those packets and countless Skype calls and instant messages originate from the United States in growing numbers, and the sender may be in the United States or abroad.⁴⁷ Likewise, it may or may not be possible to identify the sender or recipient by the e-mail addresses or phone numbers used to communicate.⁴⁸

Nor do we think of our international communications as being in any way less private than our domestic calls. Congress apparently exempted from FISA international surveillance conducted abroad because, when FISA was enacted, electronic communications by Americans did not typically cross offshore or international wires.⁴⁹ Now, of course, we do communicate internationally and our message packets may travel a long distance, even if we are corresponding by e-mail with a friend in the United States who is in the same city.⁵⁰ The location or identity of the communicants is simply not a useful marker in Internet communications. As former CIA Director General Michael Hayden said, “[t]here are no area codes on the World Wide Web.”⁵¹

44. Letter from Brian A. Benczkowski, Principal Deputy Assistant Att’y Gen., U.S. Dep’t of Justice, to Nancy Pelosi, Speaker, U.S. House of Representatives 1 (Apr. 30, 2008), *available at* <http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf>.

45. Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, EL PASO TIMES, Aug. 22, 2007, *available at* http://www.elpasotimes.com/news/ci_6685679.

46. Banks, *supra* note 7, at 1294.

47. See Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225, 234–35 (observing that due to “the dominant role of the United States in modern communications technology . . . [c]ommunications service providers in the United States end up playing host to a great deal of traffic sent and received from individuals located abroad”).

48. *Id.* at 35.

49. See *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 9 (2006) (testimony by Michael V. Hayden, Director, CIA, Office of the Director of National Intelligence), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:43453.pdf (“When [FISA] was passed, almost all local calls were on a wire and almost all long haul communications were in the air.”).

50. *Id.*

51. *Id.* at 7.

Because FISA was written to apply to broadly defined forms of “electronic surveillance”⁵² acquired inside the United States, digital technologies brought the interception of previously unregulated communications inside the FISA scheme.⁵³ In particular, digitization brought e-mail communications within the FISA scheme.⁵⁴ Because of the definition of “electronic surveillance,” even a foreign-to-foreign e-mail message could not be acquired from electronic storage on a server inside the United States except through FISA procedures.⁵⁵ While foreign-to-foreign telephone surveillance was expressly left unregulated by Congress, coverage of e-mail by FISA created an anomalous situation for investigators.

Even an exemption carved out of FISA for foreign-to-foreign e-mail would be problematic because it is often not possible to verify the location of the parties to a communication.⁵⁶ A broader authorization for e-mail surveillance would inevitably include U.S. person senders or recipients and even wholly domestic e-mail. A foreign-to-foreign e-mail exemption would effectively leave in place the requirement of individual FISA applications for overseas targets using e-mail that rely on an ISP in the United States because

52. FISA defines “electronic surveillance” as

(1) the acquisition by an electronic . . . device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic . . . device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . . ;

(3) the intentional acquisition by an electronic . . . device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic . . . device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(f), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(f)(1)–(4)).

53. See Kris, *supra* note 9, at 223 (noting that technological change from communications satellites to undersea fiber-optic cables has caused the scope of FISA to expand).

54. See Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH. L. REV. 1, 20 (2004) (noting that the USA PATRIOT Act essentially “puts email and internet communication within the purview of clandestine FISA surveillance”).

55. Kerr, *supra* note 47, at 230–32 (reporting that the provision was written to cover microphone bugs and closed-circuit television surveillance, but its original, unchanged terms apply to surveillance of foreign-to-foreign e-mail messages from inside the United States).

56. *Strengthening FISA: Does the Protect America Act Protect Americans’ Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 47 (2007) [hereinafter *Strengthening FISA*] (statement of James A. Baker, Harvard Law School, Former Counsel for the Office of Intelligence Policy and Review, United States Department of Justice).

government could neither ferret out incoming or outgoing U.S. messages in real time nor ignore those messages.⁵⁷

Changing technologies have also turned the traditional sequence of FISA processes on its head. We discovered after 9/11 that investigators could enter transactional data about potential terrorists and come up with a list that included four of the hijackers⁵⁸—a sort of reverse of the typical FISA-supported investigation. Now our intelligence agencies see the potential benefits of data mining⁵⁹—the application of algorithms or other database techniques to reveal hidden characteristics of the data and infer predictive patterns or relationships⁶⁰—as a means of developing the potential suspects that could be targets in the traditional FISA framework. In order to collect the foreign intelligence data, officials claim that they need to access the telecom switches inside the United States so that they can conduct surveillance of e-mails residing on servers in the United States.⁶¹ The mined data would necessarily include data of U.S. persons.⁶²

III. Programmatic Electronic Surveillance

A. *The Terrorist Surveillance Program*

After 9/11, President George W. Bush ordered an expanded program of electronic surveillance by the National Security Agency (NSA) that simply ignored FISA requirements.⁶³ In December 2005, the *New York Times* reported that President Bush secretly authorized the NSA to eavesdrop on Americans and others inside the United States to search for evidence of

57. Kris, *supra* note 9, at 229.

58. Kristen Breitweiser, *Enabling Danger (Part One)*, HUFFINGTON POST, Aug. 20, 2005, http://www.huffingtonpost.com/kristen-breitweiser/enabling-danger-part-one_b_5951.html. Media reports indicated that four of the hijackers had been identified in the summer of 2000 by a data-mining program called Able Danger, run by the Defense Intelligence Agency. *Id.*

59. See TECH. AND PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 45–48 (2004), available at <http://www.cdt.org/security/uusapatriot/20040300tapac.pdf> (recommending privacy protections and recognizing that data mining can “serve many useful purposes in the fight against terrorism and other crimes”). Nearly 200 data-mining programs are in use or are being developed by the government. U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2 (2004), available at <http://www.gao.gov/new.items/d04548.pdf>. This includes fourteen dedicated to analyzing intelligence and detecting terrorists. Jeff Jonas & Jim Harper, CATO Institute, Policy Analysis No. 584, *Effective Counterterrorism and the Limited Role of Predictive Data Mining* 5 (2006), available at http://www.cato.org/pub_display.php?pub_id=6784.

60. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 6 (2003).

61. See TECH. AND PRIVACY ADVISORY COMM., *supra* note 59, at 27–28 (explaining that the USA PATRIOT covers “addressing and routing” Internet communications).

62. See *id.* at 33–41 (describing the implications of government data mining on U.S. persons).

63. GLEN A. FINE, OFFICE OF THE INSPECTOR GEN. OF THE DEP’T OF JUSTICE ET AL., REPORT NO. 2009-0113-AS, (U) UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 5–7 (2009), available at <http://www.fas.org/irp/eprint/psp.pdf>.

terrorist activity without obtaining orders from the FISC.⁶⁴ Although the details of what came to be called the Terrorist Surveillance Program (TSP) have not been made public, NSA apparently monitored the telephone and e-mail communications of thousands of persons inside the United States where one end of the communication was outside the United States and where there were reasonable grounds to believe that a party to the international communication was affiliated with al Qaeda or a related organization.⁶⁵

From subsequent accounts and statements by Bush Administration officials it appears that the TSP operated in stages.⁶⁶ With the cooperation of the telecommunications companies, the NSA first engaged in wholesale collection of all the traffic entering the United States at switching stations—so-called vacuum cleaner surveillance.⁶⁷ Second, those transactional data—addressing information, subject lines, and perhaps some message content—were computer mined for indications of terrorist activity.⁶⁸ Third, as patterns or indications of terrorist activity were uncovered, intelligence officials at NSA reviewed the collected data to ferret out potential threats, at the direction of NSA supervisors.⁶⁹ Finally, the targets selected as potential threats were referred to the FBI for further investigation, pursuant to FISA, and the human surveillance ended for the others.⁷⁰

At first the Bush Administration defended the legality of the TSP vigorously, but it was an uphill struggle.⁷¹ In the face of mounting criticism and litigation challenging TSP, the Administration persuaded the FISC to take over supervision of the program,⁷² presumably within the statutory parameters of FISA. When the FISC took over administration of the TSP program in January 2007, Attorney General Alberto Gonzales advised that a FISC judge “issued orders authorizing the Government to target for collection

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

65. President George W. Bush, Press Conference on the Post-September 11 Intelligence Gathering Program (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>; see also U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 5 (2006) [hereinafter DOJ WHITEPAPER] (“The President has acknowledged that . . . he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations.”).

66. See FINE, *supra* note 63, at 15–16 (describing the layers of review that the PSP engaged in to target al Qaeda activity).

67. Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 253.

68. *Id.*

69. *Id.*

70. See FINE, *supra* note 63, at 17 (describing the FBI’s role in the TSP as a recipient of the intelligence ultimately collected).

71. See *id.* at 11–14, 20 (outlining the arguments in favor of the legality of and presidential authority to authorize the TSP).

72. See Eric Lichtblau & David Johnston, *Court to Overturn U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007, at A1 (reporting that the Bush Administration agreed to submit the NSA’s wiretapping program to the supervision of the FISA Court).

international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.”⁷³ According to the Attorney General, all surveillance that had been occurring under the TSP would now be conducted with the approval of the FISC.⁷⁴

Although the legal basis for fitting TSP inside FISA during this period has not been disclosed, the government must have persuaded at least one FISC judge to treat the international telecom switches as FISA “facilities.”⁷⁵ Because it could reasonably be argued that al Qaeda was using the switches for communications entering and leaving the United States, a few FISC orders gave the government access to nearly all of the international telecom traffic entering and leaving the United States.⁷⁶ The fact that the rest of us were using those switches at the same time was, presumably, dealt with through some version of FISA minimization procedures, where Executive Branch personnel would cull what looked like al Qaeda communications from the mass of data.⁷⁷

B. *The Protect America Act of 2007*

A different FISC judge decided in April 2007 not to continue approval of what had been the TSP under FISC supervision, and apparently determined that at least some of the foreign communications acquired in the United States pursuant to the program are subject to individualized FISA processes.⁷⁸ After a backlog of FISA applications developed, the Bush Administration successfully persuaded Congress to pass statutory authorization for programmatic surveillance outside the case-specific FISA processes.⁷⁹

The Administration emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct surveillance of foreign

73. Letter from Alberto R. Gonzales, Att’y Gen. of the U.S., to Patrick Leahy, Chairman, Comm. on the Judiciary, and Arlen Specter, Ranking Minority Member, Comm. on the Judiciary (Jan. 17, 2007), available at http://www.fas.org/irp.congress/2007_cr/fisa011707.html. He thus implicitly conceded that TSP did fall within the scope of FISA.

74. See FINE, *supra* note 63, at 30 (“Certain activities that were originally authorized as part of the PSP have subsequently been authorized under orders issued by the Foreign Intelligence Surveillance Court (FISC). The activities transitioned in this manner included the . . . ‘Terrorist Surveillance Program.’”).

75. *Id.* at 30–31.

76. FINE, *supra* note 63, at 30.

77. See Kris, *supra* note 9, at 219, 230 (explaining the government is required to adhere to specific “minimization procedures” designed to balance the government’s need to obtain intelligence against the privacy interests of Americans).

78. See *Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act Before the S. Comm. on the Judiciary*, 110th Cong. 17 (2007) (statement of J. Michael McConnell, Director of National Intelligence), http://www.dni.gov/testimonies/20070925_testimony.pdf (“[S]ome have advocated for a proposal that would exclude only ‘foreign-to-foreign’ communications from FISA’s scope.”).

79. See FINE, *supra* note 63, at 9–13 (describing key features of the PAA and the scope of its coverage).

digital communications from within the United States.⁸⁰ Yet providing statutory access to U.S. digital telecommunications switches would enable NSA to access e-mail traffic traveling to or from U.S. servers, thus opening up a vast swath of U.S. person communications for government scrutiny.⁸¹

As enacted in August 2007, the Protect America Act determined that the definition of “electronic surveillance” in FISA would not apply to surveillance of a person reasonably believed to be outside the United States.⁸² The PAA also permitted the Director of National Intelligence and the Attorney General to authorize collection of foreign intelligence from within the United States “directed at” persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States.⁸³ Because a FISA “person” may include groups or foreign powers,⁸⁴ surveillance “directed at” al Qaeda permitted warrantless surveillance of the telephones and e-mail accounts of any U.S. person if the government was persuaded that the surveillance was directed at al Qaeda.⁸⁵

The PAA thus made less onerous the determination that the target is known to be abroad. Comparing the PAA to the TSP (as characterized by Attorney General Gonzales), the main differences were that the TSP allowed surveillance of targets inside the United States, and the predicate for collection authority under the PAA was the location of the target, not his status in relation to a foreign power or terrorist organization (as it was under the TSP).⁸⁶

C. *The FISA Amendments Act of 2008*

The PAA expired by its own terms in February 2008 after Congress and the Administration failed to agree on a set of provisions that would grant broad, retroactive immunity to telecommunications firms that participated in the TSP.⁸⁷ The FISA Amendments Act of 2008, enacted in July 2008, conferred the immunity sought by the Administration and the

80. *See id.* at 5–7 (“FISA’s definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology.”).

81. *See id.* (“Thus, technological changes have brought within FISA’s scope communications that the 1978 Congress did not intend to be covered.”).

82. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c).

83. *Id.*

84. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(m), 92 Stat. 1783, 1786 (codified at 50 U.S.C. § 1801(m) (2006)).

85. Kris, *supra* note 9, at 32–33.

86. *See* David Kris, A Guide to the New FISA Bill, Part II, June 25, 2008, available at <http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html> (noting that the PAA “focuses only on the target’s location (or the government’s reasonable belief about his location) not his status or conduct as a terrorist or agent of a foreign power”).

87. Eric Lichtblau, *Rhetoric: High; Anxiety: Low*, N.Y. TIMES, Mar. 1, 2008, at A11.

telecommunications industry,⁸⁸ and it authorized until December 31, 2012, sweeping and suspicionless programmatic surveillance from inside the United States.⁸⁹

In essence, the FAA codified the PAA—with some additional wrinkles. The core of the new subtitle of FISA retains the broad-based authorization for the Attorney General and DNI to authorize jointly, for a period up to one year, the “targeting” of non-U.S. persons “reasonably believed to be located outside the United States to acquire foreign intelligence information.”⁹⁰ The FISC does not review individualized surveillance applications, and it does not supervise implementation of the program.⁹¹ The FAA does prohibit the government from “intentionally target[ing] any person known at the time of acquisition to be located in the United States.”⁹² However, the government cannot reliably know a target’s location, nor often the target’s identity.⁹³ These uncertainties, combined with the fact that the targeted person may communicate with an innocent U.S. person, mean that the authorized collection may include the international or even domestic communications of U.S. citizens and lawful residents.

Under the FAA, the Attorney General submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures.⁹⁴ Although the procedures are classified, we know that they are designed to limit the acquisition, retention, and dissemination of private information acquired during an investigation.⁹⁵ The application to the FISC must also contain a certification and supporting affidavit,⁹⁶ and “targeting procedures” designed to ensure that collection is limited to non-U.S. persons reasonably believed to be outside the United States and to prevent the intentional acquisition of communications where

88. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2441 (to be codified at 50 U.S.C. § 1881a(h)(3)) (“No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance . . .”).

89. Lichtblau, *supra* note 87; *see also* FISA Amendments Act § 403 (indicating that the codification is to expire on December 31, 2012).

90. FISA Amendments Act § 702.

91. *See* Kris, *supra* note 86 (“[T]here is no requirement that anyone—the FISA Court or the NSA—find probable cause that the target is a terrorist or a spy before (or after) commencing surveillance.”).

92. FISA Amendments Act § 702.

93. *See supra* notes 46–51 and accompanying text.

94. FISA Amendments Act § 404. The requirements for minimization in the review of individualized applications for FISA surveillance are codified in 50 U.S.C. §§ 1801(h), 1821(4). Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(h), 92 Stat. 1783, 1785–86 (codified at 50 U.S.C. §§ 1801(h), 1821(4) (2006)). Both sections direct the Attorney General to promulgate detailed minimization procedures. *Id.* The procedures are classified. *Id.*

95. *Id.* § 101. The requirements for minimization are subject to the government’s need to “disseminate foreign intelligence information.” *Id.*

96. FISA Amendments Act § 404.

the sender and all known recipients are known at the time to be located in the United States.⁹⁷ The certification and supporting affidavit must state that the Attorney General has adopted “guidelines” to ensure that statutory procedures have been complied with, that the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment, and that a significant purpose of the collection is to obtain foreign intelligence information.⁹⁸

As with the PAA and the TSP, the FAA does not limit the government to surveillance of particular, known persons reasonably believed to be outside the United States, but instead authorizes so-called “basket warrants” for surveillance and eventual data mining. In addition, non-U.S. person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.⁹⁹ Potential targets could include, for example, a non-governmental organization, a media group, or a geographic region. That the targets may be communicating with innocent persons inside the United States is not a barrier to surveillance.¹⁰⁰

For the first time, surveillance intentionally targeting a U.S. citizen reasonably believed to be abroad is subject to FISA procedures.¹⁰¹ As a practical matter, this increased protection for Americans may be illusory. The government may not target a particular U.S. person’s international communications pursuant to its programmatic authorizations, whether the person is in the United States or abroad.¹⁰² Yet officials could authorize broad surveillance, for example, of all international communications of the residents of Detroit on the rationale that they were targeting foreign terrorists who may be communicating with persons in a city with a large Muslim population.

Unlike traditional FISA applications, the government is not required to identify the facilities, telephone lines, e-mail addresses, places, or property where the programmatic surveillance will be directed.¹⁰³ Under the FAA, targeting might be directed at a terrorist organization, a set of telephone numbers or e-mail addresses, or perhaps at an entire ISP or area code.¹⁰⁴

97. *Id.*

98. *Id.*

99. FISA § 101.

100. *See* Kris, *supra* note 86 (positing that the problem was solved, or “dealt with,” via “minimization”).

101. *Compare* FISA Amendments Act § 703(a)(1), *with id.* § 702(a).

102. *See* Kerr, *supra* note 47, at 230 (revealing that FISA, as enacted in 1978, prohibited the government from intentionally targeting the phone calls of “a particular, known United States person” from either outside the United States or within it).

103. FISA Amendments Act § 702.

104. *See, e.g.*, Editorial, *Compromising the Constitution*, N.Y. TIMES, July 8, 2008, at A20 (criticizing the FAA in part because the federal government would be permitted to listen “to all calls

After a FISC judge approves the program features,¹⁰⁵ Executive Branch officials authorize the surveillance and issue directives requesting (or, through an additional court order, compelling) communications carriers to assist.¹⁰⁶ Although details of the implementation of the program authorized by the FAA are not known, a best guess is the government uses a broad vacuum-cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then NSA engages in a more particularized collection of content after analyzing mined data.¹⁰⁷

Incidental acquisition of the communications of U.S. persons inside the United States inevitably occurs due to the difficulty of ascertaining a target's location and because targets abroad may communicate with innocent U.S. persons.¹⁰⁸ The FAA does nothing to assure U.S. persons whose communications are incidentally acquired that the collected information will not be retained by the government.

Historically, minimization has been conducted during law enforcement investigations to protect against the acquisition of private information unrelated to the purpose of the criminal investigation.¹⁰⁹ The protection of civil liberties through minimization during law enforcement surveillance occurs up front rather than during retention or dissemination in part because electronic surveillance during traditional law enforcement investigations is episodic and short term. Even with traditional FISA electronic surveillance, the authorization is broader and allows for continuous and longer term monitoring, with the understanding that information irrelevant to the

to a particular area code in any other country"); Ryan Singel, *Dems Agree to Expand Domestic Spying, Grant Telecoms Amnesty*, WIRED, June 19, 2008, <http://www.wired.com/threatlevel/2008/06/dems-agree-to-e/> (indicating that under the FAA, "the intelligence community will be able to issue broad orders to U.S. ISPs, phone companies and online communications services like Hotmail and Skype to turn over all communications that are reasonably believed to involve a non-American who is outside the country"); Ryan Singel, *House Grants Telecom Amnesty, Expands Spying Powers*, WIRED, June 20, 2008, <http://www.wired.com/threatlevel/2008/06/house-grants-te/> (indicating that the FAA allows the NSA "to order phone companies, ISPs and online service providers to turn over all communications that have one foreigner as a party to the conversation").

105. FISA Amendments Act § 702. FISC approval of a written certification from the Attorney General and DNI must occur prior to implementation of the authorization for surveillance, unless the same officials determine that time does not permit the prior review, in which case the authorization must be sought as soon as practicable, but not more than seven days after the determination is made. *Id.*

106. *Id.*

107. See Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 253 (describing the NSA process of "content filtering" and "traffic analysis").

108. *Id.* at 252.

109. See *Berger v. New York*, 388 U.S. 41, 58–59 (1967) (striking down an electronic surveillance statute because it allowed acquisition of "the conversations of any and all persons coming into the area covered by the device . . . indiscriminately and without regard to their connection with the crime under investigation").

investigation will be collected.¹¹⁰ Thus, according to a 2002 opinion of the FISC,¹¹¹ the government conducts FISA minimization after processing (including transcription, translation, and analysis), and the retained foreign intelligence enters an indexed storage system for retrieval.¹¹² In explaining the minimization challenges inherent in foreign intelligence surveillance, the FISC stated in 2002, “[g]iven the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots.”¹¹³ In addition, unlike the targets of FISA surveillance, Title III targets eventually receive notice that they have been subject to surveillance. They may sue for Fourth Amendment violations, seek to suppress the evidence in a prosecution, or both.¹¹⁴ Traditional FISA minimization protects only nonpublic information concerning U.S. persons who have not consented to acquisition, retention, or dissemination of their personal information,¹¹⁵ and FISA permits the government to retain all information that could be considered foreign intelligence.¹¹⁶

The generic FISA minimization requirements were not modified in the FAA to accommodate the surveillance of individual targets through programmatic surveillance.¹¹⁷ The FAA requires that the Attorney General and the DNI certify that minimization procedures have been or will be submitted for approval to the FISC prior to, or within seven days following, implementation.¹¹⁸ However, the FISC does not review the implementation of minimization procedures or practices for the programmatic surveillance it approves, and FISA permits the government to retain and disseminate information relating to U.S. persons so long as the government determines that it

110. See *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).

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

112. *Id.* at 617–18; see also *In re Sealed Case* 310 F.3d at 740 (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).

113. *In re Sealed Case*, 310 F.3d at 741.

114. Compare 18 U.S.C. § 2518(9) (2006), with Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 106(f), 92 Stat. 1783, 1794 (codified at 50 U.S.C. § 1806(f)).

115. See FISA § 101(h)(1) (defining minimization procedures to mean “specific procedures . . . designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons”).

116. *In re All Matters*, 218 F. Supp. 2d at 617–18. Early experience with minimization under FISA is reviewed in Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs Are Doing Their Jobs*, 12 RUTGERS L.J. 405 (1981).

117. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2439 (to be codified at 50 U.S.C. § 1881a(e)).

118. FISA Amendments Act § 702.

is “foreign intelligence information.”¹¹⁹ By implication, the government may compile databases containing foreign intelligence information from or about U.S. persons, retain the information indefinitely, and then search the databases for information about specific U.S. persons.

Viewing minimization as it evolved from Title III to traditional FISA and to the FAA, the original objective—preventing the collection, retention, or dissemination of private information—has been seriously compromised, or so it seems from the public record. The combination of allowing the government to use the foreign intelligence trump card to hold or disseminate information and the lack of judicial oversight of how private communications are filtered out leaves the minimization mechanism short of meeting its goals for programmatic FISA surveillance. Because FISA minimization is already focused on retention and dissemination and not on acquisition, it should be relatively easy to reform FAA minimization to insert controls on executive discretion and assign a monitoring function to the FISC.

The FISC has described its role in authorizing and reviewing surveillance conducted under the FAA as “narrowly circumscribed.”¹²⁰ The FISC must approve an order for programmatic surveillance if it finds that the government’s certification “contains all the required elements,”¹²¹ that the targeting procedures are “reasonably designed” to target non-U.S. persons,¹²² and that the targeting and minimization procedures are consistent with the FAA and the Fourth Amendment.¹²³ The FISC does not supervise the implementation of the targeting and thus does not review the efficacy of specific surveillance targets.

Long-term congressional authorization for programmatic surveillance marks a stark change in FISA. The FAA permits collection without any showing of individualized suspicion (except for U.S. persons targeted abroad) even where collection of U.S. citizens’ communications is the foreseeable consequence of the program orders.¹²⁴ It may be that individualized FISA applications and their foreign agency or lone-wolf probable-cause determinations are relics of the pre-digital age. Congress and the Executive Branch should confront the realities of digital surveillance and develop approval procedures, minimization safeguards, and judicial and legislative oversight mechanisms to govern the use of data mining and related surveillance techniques to better insure that programmatic surveillance protects our security and our liberties.

119. See FISA § 101(h)(2) (indicating that nonpublicly available information can be disseminated in a manner that identifies a U.S. person without their consent when such person’s identity “is necessary to understand foreign intelligence information or assess its importance”).

120. *In re* Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008).

121. FISA Amendments Act § 702.

122. *Id.*

123. *Id.*

124. *Id.*

IV. Implementation of Programmatic Surveillance

A. *The Directives Decision*

On January 15, 2009, the FISCRC made public portions of its August 22, 2008, decision, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*.¹²⁵ In *Directives*, the FISCRC upheld the constitutionality of directives in pursuit of programmatic surveillance issued to an unnamed telecommunications company pursuant to the temporary Protect America Act.¹²⁶ Because the FAA follows the basic thrust of the PAA, the opinion foreshadows the court's view of the now-codified procedures for programmatic surveillance. The telecom followed a statutory provision and challenged orders compelling it to assist with the acquisition of foreign intelligence where the target was a U.S. person reasonably believed to be outside the United States.¹²⁷ The orders were made following a joint determination by the DNI and the Attorney General that the acquisition satisfied a series of criteria, including minimization procedures.¹²⁸

In its heavily redacted opinion—only the second one publicly issued in its thirty year history—the FISCRC held that there is a foreign intelligence exception to the Fourth Amendment warrant requirement, based on the “special needs” doctrine, at least in the “defined context” of cooperation directives to a telecom company.¹²⁹ The exception is available for the programmatic purpose of the surveillance because the acquisition goes “beyond ordinary crime control” and foreign intelligence surveillance about “overseas foreign agents” is “particularly intense.”¹³⁰ Fourth Amendment reasonableness was met in this case through a variety of safeguards found outside the statute. The telecom argued that the collection activities would inevitably lead to incidental collection from nontargeted U.S. persons, but, without further explanation or support, the FISCRC characterized the concern as “overblown.”¹³¹ If incidental, said the court, the collections do not violate the Fourth Amendment.¹³²

Relying on the FISCRC's own 2002 *In re Sealed Case* decision,¹³³ the telecom argued that the procedural protections provided by the FAA were insufficiently analogous to protections found in the earlier version of FISA, including a particularity requirement, prior judicial review for probable cause

125. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1017–18 (FISA Ct. Rev. 2008).

126. *Id.* at 1011–12.

127. *Id.* at 1006.

128. *Id.* at 1007.

129. *Id.* at 1010–12.

130. *Id.* at 1011.

131. *Id.* at 1015.

132. *Id.*

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

of foreign agency, and proxies for any omitted protections.¹³⁴ Despite the absence of these protections, in its 2008 decision the FISC supported the government's contention that Fourth Amendment reasonableness could be constructed from:

at least five components: targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and [redacted text] procedures [redacted text] outlined in an affidavit supporting the certifications.¹³⁵

The FISC concluded that the telecom presented no evidence of harm in this instance. According to the court, particularity and prior judicial-review concerns are “defeated by the way in which the statute has been applied.”¹³⁶ According to the court, classified procedures approved by the Attorney General, when “combined with the PAA’s other protections,” and those provided in the Executive Order “are constitutionally sufficient compensation for any encroachments.”¹³⁷ The next two subsections evaluate the court’s Fourth Amendment analysis.

1. Special Needs.—The special-needs doctrine is a limited exception to the Fourth Amendment warrant requirement. It grew out of searches or surveillance as part of programs that were developed for purposes other than enforcing the criminal laws—searches for drugs in school lockers or immigration checkpoints at our nation’s borders, for example.¹³⁸ To invoke the doctrine, the government must show that the primary purpose of its surveillance is something other than law enforcement and that following the warrant and probable cause requirements is impracticable.¹³⁹ If the special needs are accepted, the result is to exempt searches or surveillance authorized by the program from the warrant requirement, leaving reasonableness alone as the more general Fourth Amendment measure.

Following the USA PATRIOT Act amendments to FISA in 2001, the FISC relied in part on the special-needs doctrine to uphold Department of Justice guidelines that permitted criminal investigators to assume lead roles

134. *In re Directives*, 551 F.3d at 1013.

135. *Id.*

136. *Id.*

137. *Id.*

138. *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (approving warrantless searches that were designed to meet the government’s “special needs, beyond the normal need for law enforcement” (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987))).

139. *See Ferguson v. City of Charleston*, 532 U.S. 67, 81–86 (2001) (declaring arrests made pursuant to hospital urine tests unconstitutional because of the policy’s law enforcement purpose); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41–47 (2000) (invalidating “drug checkpoints” because the program’s primary purpose was to uncover evidence of ordinary criminal wrongdoing); *Griffin*, 483 U.S. at 880 (upholding the supervision of prisoners as a “special need” justifying departure from the warrant process).

in FISA-authorized surveillance so long as “a significant purpose” of the investigation included collecting foreign intelligence.¹⁴⁰ Arguably, the special-needs doctrine should not have been applied in the traditional FISA setting to justify individually targeted electronic surveillance after the “significant purpose” amendment in 2001.¹⁴¹ Although intelligence and law enforcement investigations often overlap in pursuit of national-security or counterterrorism targets, law enforcement officials may exploit the more government-friendly FISA processes and avoid traditional law enforcement rules for securing a warrant when they, and not intelligence investigators, are in charge of an investigation and, from the beginning, are working to build a case for prosecution.¹⁴²

In any case, following the 2002 *In re Sealed Case* FISC decision, the amended statute has been construed to permit the government to engage in “special needs” surveillance when the overriding objective of the surveillance is to gather evidence for prosecution.¹⁴³ The “significant purpose” qualifier applies to programmatic surveillance authorized under the FAA.¹⁴⁴ The use of programmatic surveillance to build a criminal case, such as a large criminal conspiracy, is at least as likely in these instances as in individual FISA applications. Although I continue to doubt the wisdom and lawfulness of the “significant purpose” standard, in the last section of the Article, I propose to accept programmatic surveillance for foreign intelligence as a “special needs” category so long as a series of safeguards are embedded in the system, including a review to assess the importance of the foreign intelligence objective of the surveillance.

2. *Reasonableness.*—The substitutions of individualized FISC review of applications for a traditional warrant and a specialized foreign intelligence related probable cause standard have been construed by nearly every court that has considered their constitutionality as adequate for Fourth Amendment

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

141. *See Banks*, *supra* note 7, at 1282 (asserting that the application of the special-needs doctrine after the “significant purpose” amendment could allow the program to be used even when its sole purpose is the collection of evidence for prosecution without any version of a probable-cause requirement).

142. *See id.* at 1269–70 (noting that FISA should be unavailable if the purpose of the investigation is to prosecute because of FISA’s requirements and the protections of the First, Fourth, and Sixth Amendments).

143. *See Mayfield v. United States*, 504 F. Supp. 2d 1023, 1032 (D. Or. 2007) (holding that “the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes”), *rev’d*, 588 F.3d 1252 (9th Cir. 2009) (declining to address the question of whether the challenged provisions of FISA, as amended by the USA PATRIOT Act, was unconstitutional).

144. *Id.*

purposes.¹⁴⁵ The programmatic orders are so dramatically different from the thirty-year FISA experience, however, that their suspicionless targeting procedures may not be reasonable in Fourth Amendment terms.

In the circumstances of foreign intelligence surveillance designed to counter threats of terrorism and to protect the national security, it is no longer realistic to argue that the Warrant Clause and its traditional law enforcement warrants and the criminal law version of probable cause should apply in the foreign intelligence context, at least where the government demonstrates that the foreign intelligence sought is important to an ongoing counterterrorism investigation and that it is impractical to seek a warrant. As such, the FISCR holding in *Directives* that there is a foreign intelligence exception to the Warrant Clause is not particularly important. Yet the wooden and pasted-together quality of the court's reasonableness analysis is unfortunate, particularly since reasonableness is the only remaining Fourth Amendment criterion for assessing the programmatic surveillance.

The court purported to make a fact-based decision about reasonableness, as applied to the telecom and the directive it was issued.¹⁴⁶ Ironically, reasonableness was constructed by the court in part from minimization, but we have no idea what the minimization entailed. The facts are opaque due to classification and, whatever they reveal, are based on generic authorization for collection of personal information, on targeting procedures that may significantly overcollect U.S. person information, and are developed solely by the government without opportunity for adversarial testing. The FISCR must have recognized that it was working with especially limited statutory criteria for reasonableness. As a result, the FISCR reached outside the FAA to an executive order and an affidavit and relied on the assumed good faith of the implementers in deciding that there were adequate protections for the telecom.¹⁴⁷

As an illustration that challenges to electronic surveillance in the foreign intelligence realm should not excuse a thorough reasonableness review, a panel of the Second Circuit affirmed several convictions in the Africa Embassies bombings prosecutions after a much more fulsome and thoughtful assessment of the Fourth Amendment.¹⁴⁸ While the Second Circuit panel began with similar "totality of the circumstances" and balancing quotes from

145. See *In re Sealed Case*, 310 F.3d at 742 ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). But see *Mayfield*, 504 F. Supp. 2d at 1023.

146. See *In re Sealed Case*, 310 F.3d at 377–79.

147. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1014–15 (FISA Ct. Rev. 2008). In what the FISCR calls a "parting shot," the telecom raised what the court called "a specific privacy concern." *Id.* at 1015. The court mentioned it only to task the Executive with notifying the telecom if that concern, whatever it is, arises. We cannot know whether the telecom was drawing attention to the inevitability of overcollection, either in general or specifically in this case. *Id.*

148. *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157 (2d Cir. 2008).

landmark precedents cited by the FISCR,¹⁴⁹ its analysis carefully probed the factual record. Concerning the telephone surveillance conducted as part of the investigation of the bombings, the court found significant privacy invasions during the year-long surveillance, accompanied by limited efforts at minimization.¹⁵⁰ In balancing the intrusion against the government's need to conduct electronic surveillance, the court took into account: the difficulties of pinpointing surveillance of diffuse organizations like al Qaeda; the problems inherent in sorting through much irrelevant information in pursuit of foreign intelligence; the tendency of organizations such as al Qaeda to communicate in code; and the need to sift through foreign languages in finding relevant intelligence.¹⁵¹ No similar fine-grained analysis accompanied the FISCR *Directives* decision.

The FAA enables the government to overhear Americans' most intimate conversations, for periods up to one year, and there is no judicial gatekeeper of administrative discretion—the agencies decide which communications to monitor. Where targeting and minimization requirements monitored by the FISC help show reasonableness in the traditional FISA setting, programmatic FISA surveillance leaves targeting and minimization so unbounded that the two features do little to assure Fourth Amendment reasonableness. Reasonableness requires a careful evaluation of the government's conduct, and neither the FAA nor the *Directives* opinion contain the necessary review.

One rejoinder to the *Directives* court's scattershot construction of reasonableness is that Congress improved the scheme in enacting the permanent FAA one year later by requiring probable cause of foreign agency for surveillance targeting U.S. persons abroad or intentional targeting of U.S. persons domestically.¹⁵² Still, incidental collection of U.S. person communications inside the United States was not addressed by the FAA, and the *Directives* decision does not assess the reasonableness of such collection.

The FISCR conclusion that “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful”¹⁵³ faithfully parrots Fourth Amendment doctrine¹⁵⁴ but fails to respond to the unique circumstances of programmatic FISA surveillance. Viewing the public record in the *Directives* case, it is impossible to know to what extent the telecom had shown harmful effects of incidental collections.

149. *Id.* at 172 (quoting *Samson v. California*, 547 U.S. 843, 848 (2006)).

150. *Id.* at 175.

151. *Id.* at 175–76.

152. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2448–51 (to be codified at 50 U.S.C. §§ 1881b–1881c).

153. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008).

154. *Id.* at 1015 (citing, *e.g.*, *United States v. Kahn*, 415 U.S. 143, 157–58 (1974)). In *United States v. Butenko*, 494 F.2d 593, 608 (1974), a review of warrantless surveillance for foreign intelligence purposes found that incidental collection that infringes privacy should be reviewed as part of Fourth Amendment reasonableness.

In any case, the FISC did not acknowledge just how significant an intrusion the “incidental” collection could be.

B. Implementing the FAA

A lawsuit filed by the ACLU challenging the constitutionality of the FAA was dismissed on standing grounds in August 2009.¹⁵⁵ Meanwhile, following a periodic review of the procedures and directives implemented following enactment of the FAA, the Justice Department and DNI reported to the FISC in April 2009 that the NSA had been engaging in significant and systematic overcollection of the domestic e-mail messages of Americans.¹⁵⁶ Though apparently inadvertent, the lapses were headline news and prompted congressional investigations.¹⁵⁷ Unsurprisingly, as the NSA uses telecom switching stations and its satellites to intercept millions of messages, one apparent cause of the overcollection of domestic e-mail messages is the ongoing difficulty of determining the location of the surveillance target.¹⁵⁸

As investigations were launched, some members of Congress disputed the contention that the overcollection was inadvertent.¹⁵⁹ Representative Rush Holt, D-N.J., Chair of the House Select Intelligence Oversight Committee, worried that “the people making policy don’t understand the technicalities.”¹⁶⁰ Intelligence officials told the *New York Times* that the NSA exceeded its statutory authorities in implementing eight to ten separate orders issued by the FISC since enactment of the FAA.¹⁶¹ Because each order could permit collection of hundreds or thousands of phone numbers or e-mail addresses, millions of individual communications could have been intercepted, some portion of which would have been domestic communications by U.S. persons.¹⁶²

155. *Amnesty Int’l USA v. McConnell*, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009).

156. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 6, 2009, at A1.

157. James Risen & Eric Lichtblau, *Extent of E-mail Surveillance Renews Concerns in Congress*, N.Y. TIMES, June 17, 2009, at A1.

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*; see also Scott Horton, *Operation Pinwale*, HARPER’S MAG., June 18, 2009, available at <http://harpers.org/archive/2009/06/hbc-90005232> (describing a database code named Pinwale that allegedly contains a large volume of Americans’ e-mail messages collected by the NSA).

V. Benchmarks for Reform

A. *Revising Targeting*

“If the government genuinely cannot determine a person’s location, it makes no sense to use geography as a trigger for FISA’s warrant requirements.”¹⁶³

One problematic feature of the FAA is, notwithstanding all the amendments to FISA over the years, that the legislation *follows* the thirty-year FISA model of focusing on targets and their location for the purposes of authorizing and conditioning surveillance and data collection. From the government’s perspective, the disadvantage of relying on the location of the target as a basis for conducting lawful surveillance was mitigated when the FAA changes provided that the government had only to reasonably believe that the target is abroad.¹⁶⁴ However, one inevitable problem with the relaxed standard is that, given the unreliability of the location identifier, more warrantless surveillance of persons inside the United States will occur.

The technical problems of knowing an individual’s location when an electronic communication is sent or received may also be lessened when implementing FAA surveillance through an expansive interpretation of the FISA definition of “person.” The term is broad enough to include diffuse non-state groups such as al Qaeda.¹⁶⁵ The “reasonably believe” standard presumably may be met because, at any one time, some persons affiliated with al Qaeda may be in the United States and some may be abroad; some may be U.S. persons and some may not.

In place of these workarounds, it is time to replace location of a target as a marker for regulation. Just as our national security interests and threats transcend borders, our personal liberties, including free expression and privacy, are expressed globally. If neither security nor personal freedoms are advanced by adhering to the traditional dividing line that prescribes authorities for warrantless electronic surveillance, it is time to find another approach.

One problem, of course, is that foreigners abroad are consumers of U.S. cyberspace. When corresponding with another foreigner, these persons are unprotected by the Fourth Amendment if they lack other ties with the United

163. Kris, *supra* note 9, at 237.

164. *See id.* at 229 (noting that the amendments, pending at the time, only require the “government’s reasonable belief about [a target’s] location,” as opposed to the more demanding requirement of the target’s “status . . . as a terrorist or agent of a foreign power”).

165. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(m), 92 Stat. 1783, 1786 (codified at 50 U.S.C. § 1801(m) (2006)) (defining “person” as “any individual, including any officer or employee of the Federal government, or any group, entity, association, corporation, or foreign power”).

States.¹⁶⁶ There is no reason to limit our intelligence agencies in surveillance of those communications, and the FAA facilitates that collection. Yet if we unleash surveillance at U.S. switches, our laws and policies have not yet devised a way to prevent them from gaining access to the everyday communications of Americans, the dominant consumers of those switches.

I agree with Orin Kerr that much modern surveillance is “data-focused rather than person-focused.”¹⁶⁷ I also agree with Fred Cate that “[t]he absence of a legal regime governing data mining not only fuels privacy concerns, but also runs the risk of compromising the very objectives that data mining is designed to serve.”¹⁶⁸ Where location, identity, or both of a target are unknown, I, like Kerr, recommend a predicate for surveillance that focuses on the nature of the information sought. Whether the electronic surveillance technique consists of collection followed by data mining or collection accompanied by filtering, and whether the information collected is characterized as “terrorist intelligence information,” as Kerr labels it,¹⁶⁹ or foreign intelligence that bears directly on important national-security or counterterrorism objectives,¹⁷⁰ the government should be permitted to conduct warrantless electronic surveillance if it can demonstrate in advance to the FISC that the information cannot be obtained through a less intrusive means and that it likely will collect what is sought.

Another approach would provide a uniform standard for any collection technique that would require a Fourth Amendment warrant if undertaken for law enforcement purposes in the United States.¹⁷¹ Following the current FAA, FISC approval would be required, subject to a probable cause showing that the surveillance will reveal the information sought, if a U.S. person is targeted for FISA surveillance anywhere, if a target is known to be in the United States, or if officials know in advance that a communication is wholly domestic.¹⁷² All other categories of collection could be authorized by Executive Branch officials. Collection of non-content information, such as addressing information, would be permitted after administrative review to ascertain that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence. Electronic

166. See *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990) (rejecting a Fourth Amendment claim based on the fact that the searched person had “no voluntary attachment to the United States”).

167. Kerr, *supra* note 47, 232–33.

168. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 437 (2008).

169. Kerr, *supra* note 47, at 238.

170. Judge Posner would define the predicate for programmatic surveillance narrowly. “[T]hreats to national security” would include only “threats involving a potential for mass deaths or catastrophic damage to property or to the economy.” Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 258.

171. See Kris, *supra* note 9, at 235–36 (suggesting changes to the FAA that would apply to communications between a sender and receivers all located in the United States).

172. *Id.*

surveillance of the contents of communication of other categories of targets could be administratively approved following a showing of probable cause that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence, that the information cannot be obtained through a less intrusive means, and that it is likely that the surveillance technique proposed will collect the information.¹⁷³ These or similar reforms could eliminate the “agent of a foreign power” and “lone wolf” categories altogether.

B. What Happens with the Collected Data?—Minimization and Related Issues

We believe the retention and use by IC organizations of information collected under . . . FISA should be carefully monitored.¹⁷⁴

While simplifying the basic targeting and presurveillance approval requirements will improve the overall FISA scheme, so much would be left to the discretion of unelected officials that FISA collection reforms should also focus on postcollection controls. The quotation above from the Inspectors General of DOD, DOJ, CIA, NSA, and ODNI is taken from the conclusions of their report on Bush Administration surveillance activities.¹⁷⁵ Following their lead, minimization should be enhanced for programmatic surveillance to make less likely the misuse of the massive collection of personal information about U.S. persons. Whether or not Fourth Amendment jurisprudence recognizes the collected information as part of our reasonable expectation of privacy,¹⁷⁶ Congress should impose limits on the retention, use, and dissemination of the information collected through FISA programmatic orders or directives.

Every FAA decision bearing on specific intelligence targets is made by Executive Branch officials and is not subject to review by the FISC or another judge.¹⁷⁷ Prior identification of targets to a judge protects innocent third parties from being swept up in the surveillance and enforces the

173. Kerr, *supra* note 47, at 238–39.

174. FINE, *supra* note 63, at 38.

175. *Id.* at 3.

176. See *Warshak v. United States*, 490 F.3d 455, 473–76 (6th Cir. 2007) (finding that individuals have a “reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP” and thus that the government must provide notice and an opportunity to be heard before compelling the ISP to turn over the e-mails to the government), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc); see also Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 82–83 (2005) (advocating due process protections in data mining).

177. The FISA Court only reviews targeting and minimization procedures to ensure that they meet the statutory requirements and the Fourth Amendment, and the court only reviews certifications as a matter of form, to ensure that they “contain[] all the required elements.” Kris, *supra* note 86, at 230 (citing FISA Amendments Act, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2444 (to be codified at 50 U.S.C. § 1881a(i)(3)(A)–(B))).

hallmark predicate for government surveillance—individualized suspicion.¹⁷⁸ The breadth of FAA orders and determinations permits vacuum-cleaner-like collection from telecom switches, for example.¹⁷⁹ Once collected, executive officials cull through the data in pursuit of suspicious indicators that merit further investigation.¹⁸⁰ False positives are one inevitable result. Another is the potential for abuses of stored data.¹⁸¹

How do officials determine to look more closely at individualized pieces of the traffic? Apparently NSA uses algorithms that purport to identify terrorist suspects out of the vacuumed mass of data.¹⁸² How exactly could such a data-driven process sort the innocuous call to me from my Muslim friend abroad from one that is worthy of further investigation? Is the limited, follow-on surveillance performed by humans then a minimal intrusion that we should be prepared to accept if we are assured that the brief surveillance will end and a traditional FISA application would follow if further electronic surveillance is deemed worthwhile?¹⁸³

Under traditional, individualized FISA processes, “specific procedures” for minimization must be promulgated by the Attorney General and filed with the FISC for every individual target, “to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”¹⁸⁴ The case-specific procedures are classified.¹⁸⁵ In these cases, the minimization itself is supervised by the FISC during the course of surveillance,¹⁸⁶ and the court may modify the procedures and order that the

178. See, e.g., Cate, *supra* note 168, at 480, 487 (arguing that prior judicial authorization in data mining would help better balance security with privacy concerns).

179. See Mark Williams, *The Total Information Awareness Project Lives On*, TECH. REV., Apr. 26, 2006, available at <http://www.technologyreview.com/communications/16741> (explaining that when the NSA practices automated data mining, FISA requirements are inapplicable because it is not a search of a specific individual).

180. Cate, *supra* note 168, at 473–74.

181. *Id.* at 471–80.

182. See Williams, *supra* note 179 (stating that the NSA uses electronic analysis and content filtering to apply “highly sophisticated search algorithms and powerful statistical methods . . . [to] search for particular words or language combinations that may indicate terrorist communications”).

183. See K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, 8 N.Y.U. REV. L. & SECURITY, NO. VII SUPPLEMENTAL BULL. ON L. & SECURITY 3, 5–6 (2006) (so advocating).

184. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(h)(1), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(h)(1) (2006)). The procedures are also sent to the Intelligence Committees in Congress. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702(f)(2)(A), 122 Stat. 2436, 2439 (to be codified at 50 U.S.C. § 1881a(1)(1)(B)).

185. FISA § 106(f).

186. *Id.* § 105(d)(3); Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 304(c)(3), 108 Stat. 3423, 3448 (codified at 50 U.S.C. § 1824(d)(3) (2006)).

modified procedures be followed if it finds that the proposed procedures do not satisfy the FISA definition.¹⁸⁷

By focusing on what the collected information may be used for, FISA and the FISC, until the FAA, provided a useful, albeit opaque, mechanism to ensure the accountability of the collection scheme. To be sure, the government could use and disseminate information about a person who was not the target of the approved surveillance, but whose information was collected inadvertently.¹⁸⁸ In addition, the “consistent with” clause provides a hedge for the government to disclose to law enforcement officials or, presumably, to anyone else foreign intelligence information.¹⁸⁹ Indeed, in discussing the retention stage of minimization, the publicly released 2002 FISC opinion quotes the following standard from the *Justice Department Standard Minimization Procedures for U.S. Person Agent of a Foreign Power*: “communications of or concerning United States persons *that could not be* foreign intelligence information or are not evidence of a crime . . . may not be logged or summarized.”¹⁹⁰ Because minimization “is required only if the information ‘*could not be*’ foreign intelligence,”¹⁹¹ the standard is already extremely friendly to the government.

By its nature, the FAA shifts nearly all the burden of civil liberties protection to postcollection minimization, and there is no publicly known mechanism for tailoring minimization to these new conditions. Executive Branch personnel select which communications are retained and, thus, logged and indexed in some way for ease of retrieval, all without judicial supervision.¹⁹² Relying on the default requirements, by following FAA minimization procedures the government could compile databases of collected information, maintain them, and search them later for information about U.S. persons.¹⁹³

Minimization requirements should be reviewed alongside the predictive abilities of the data-mining methods employed in programmatic

187. FISA § 105(a)(5); Intelligence Authorization Act § 304(a)(5).

188. See *supra* notes 114–17 and accompanying text.

189. See *supra* note 184 and accompanying text.

190. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

191. *Id.*

192. It is, of course, also true that the failure of the government to log or index a communication that made that record practically inaccessible when FISA was enacted would not stand in way of retrieval of the record today if officials employed their search software. See DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS 9-22 to -24 (2007) (describing “tensions” between retention and discovery in criminal cases, where useable files are disclosed to the defendant in compliance with *Brady*, including non-pertinent audio files that should have been destroyed or rendered useless following minimization). In other words, even information minimized following traditional FISA practices might still be accessible to the government. *Id.*

193. See *supra* notes 115–17 and accompanying text.

surveillance.¹⁹⁴ In 2008, a committee of the National Research Council found that “automated identification of terrorists through data mining is neither feasible as an objective nor desirable as a goal of technology development efforts.”¹⁹⁵ Apart from the serious privacy intrusions that are an incident of data mining, the committee found that the questionable quality of the data in countering terrorism (in countering terrorism, much of the information collected is unreliable or has unclear meaning),¹⁹⁶ its propensity to lead to false positives, the vulnerability of data mining to countermeasures, and the paucity of scientific evidence supporting data mining argue that, at most, the techniques should be used as a “preliminary screening method for identifying individuals who merit additional follow-up investigation.”¹⁹⁷ Employed only as a “preliminary screening method,”¹⁹⁸ “any information-based counterterrorism program of the U.S. government should be subjected to robust, independent oversight.”¹⁹⁹ For programmatic surveillance pursuant to FISA, their recommendation translates into rigorous minimization focused on retention and dissemination, supervised by the FISC.

The National Research Council acknowledged that traditional minimization “has been rendered largely irrelevant in recent years as technology and applications have evolved so that vast streams of data are recorded and stored, rather than just limited, relevant elements. . . . [E]ven irrelevant data are routinely retained by the government indefinitely.”²⁰⁰ The Council recommends that “[w]henver practicable” personal identifying information should be “removed, encrypted, or otherwise obscured”²⁰¹ before retention or dissemination.

Whether or not required by the Fourth Amendment, minimization that protects against undue retention and dissemination would serve the particularity values that have long been central to Fourth Amendment

194. Daniel J. Solove, *Data Mining and the Security–Liberty Debate*, 75 U. CHI. L. REV. 343, 352–53 (2008).

195. COMM. ON TECHNICAL AND PRIVACY DIMENSIONS OF INFO. FOR TERRORISM PREVENTION AND OTHER NAT’L GOALS ET AL., NAT’L RESEARCH COUNCIL OF THE NAT’L ACADEMIES, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 3–4 (2008) [hereinafter PROTECTING INDIVIDUAL PRIVACY], available at http://epic.org/misc/nrc_rept_100708.pdf.

196. Cate, *supra* note 168, at 469–70.

197. PROTECTING INDIVIDUAL PRIVACY, *supra* note 195, at 4. The committee offered a detailed framework for prospective development of data-mining programs to combat terrorism. *Id.* at 44–66. *But see* *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 14 (2007) (testimony by Kim Taipale, Founder and Executive Director, Center for Advanced Studies in Science and Technology Policy), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:33226.pdf (arguing that data mining for counterterrorism is a useful investigative tool that may be tailored to meet government needs and protect privacy).

198. PROTECTING INDIVIDUAL PRIVACY, *supra* note 195, at 4.

199. *Id.* at 5.

200. *Id.* at 55.

201. *Id.*

reasonableness. Since 1976, the Supreme Court has held that there is no reasonable expectation of privacy in data held by a third party.²⁰² Courts have reasoned that, by transferring the information to a third party, such as a bank, phone company, or ISP, the consumer has no reasonable expectation of privacy that prevents the company from sharing the information with the government.²⁰³ The evolving third-party-records doctrine has, in turn, provided the legal basis for a variety of law enforcement and national security-related data-collection schemes by the government, including collection authorized by FISA.²⁰⁴

Because data mining and its techniques are employed after collection, the Fourth Amendment may not control what government does to use or store the collected information.²⁰⁵ Although there are signs that some courts are beginning to question the efficacy of the third-party doctrine in the context of data mining for national-security and counterterrorism purposes,²⁰⁶ a reversal of the Supreme Court rule is unlikely anytime soon.²⁰⁷ Nor would a judicial reversal respond to the shortcomings in regulating data mining for foreign intelligence purposes.²⁰⁸ Instead, Congress and investigating agencies should adopt controls on the use of data mining for foreign intelligence purposes.

During the pre-enactment hearings on FISA more than thirty years ago, Congress recognized that there are “a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition.”²⁰⁹ The FISA practice of retaining foreign intelligence has relied on selective logging and indexing of information.²¹⁰ The FISC, in its 2002 *In re All Matters* opinion, closely examined the retention stage, and

202. See *United States v. Miller*, 425 U.S. 435, 442 (1976) (holding a bank customer had no expectation of privacy in checks and deposit slips held by a bank); see also *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (holding there is no expectation of privacy when a pen register is installed on phone company property at the company’s office because people do not reasonably believe there is an expectation of privacy when they “convey” a dialed phone number to the phone company).

203. See *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 742 (both reasoning that the expectation of privacy vanishes when a person voluntarily submits data to a third party).

204. See *Cate*, *supra* note 168, at 454–60 (setting out the Court’s decisions in *Miller* and *Smith* and applying that line of cases today).

205. Solove, *supra* note 194, at 356–57 (finding that the third-party doctrine severely limits Fourth Amendment protections where the government mines data voluntarily given to companies by their customers).

206. Cf. *Warshak v. United States*, 490 F.3d 455, 473, 482 (6th Cir. 2007) (finding Fourth Amendment protection against the government’s warrantless subpoena of e-mails transmitted through a commercial ISP where the fact that it was not the ISP’s normal practice to review e-mails supported users’ reasonable expectation of privacy), *vacated*, 532 F.3d 521 (6th Cir. 2008).

207. *Cate*, *supra* note 168, at 460.

208. *Id.*

209. H.R. REP. NO. 95-1283, pt. 1, at 56 (1978).

210. See *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002) (outlining the principal steps in the minimization process), *abrogated by In re Sealed Case*, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

concluded that the critical determination is when “a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine intelligence activities or international terrorism.”²¹¹ If the case agent decides that there is no foreign intelligence information in what is being reviewed, minimization would leave the recorded information off the indexing table: “if recorded[,] the information would not be indexed, and thus become non-retrievable[;] if in hard copy[,] from facsimile intercept or computer print-out[,] it should be discarded[;] if on re-recordable media[,] it could be erased[;] or if too bulky or too sensitive, it might be destroyed.”²¹² Over time, criminal appeals where FISA surveillance was alleged to have been conducted unlawfully revealed that minimized information may nonetheless have been recorded and not destroyed and may remain in some electronic format available for retrieval.²¹³ In programmatic surveillance, NSA personnel likely substitute for the FBI case agent.²¹⁴ The magnitude of the minimization corpus has changed so much that guidelines for ferreting out material to be minimized and for administrative review of retention decisions should be promulgated.

In a September 2007 letter to the House Intelligence Committee, the Civil Liberties Protection Officer for the ODNI explained that minimization procedures then in place at NSA, while not identical to those used for the PAA or FAA, “provide[d] general guidance for the types of processes and requirements involved with minimization.”²¹⁵ Summarizing a declassified version of United States Signals Intelligence Directive 18 (USSID 18), the letter notes that U.S. person communications “may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement;”²¹⁶ identities of U.S. persons “are generally redacted . . . and replaced with generic terms”;²¹⁷ and U.S. person identities may be released if “necessary to understand foreign intelligence information or assess its importance.”²¹⁸ The letter emphasizes that, in addition to the ODNI

211. *Id.*

212. *Id.*

213. KRIS & WILSON, *supra* note 192, at 9–23.

214. See OFFICE OF DIR. OF NAT’L INTELLIGENCE, ELECTRONIC FRONTIER FOUNDATION FINAL RESPONSE (2007), available at http://www.dni.gov/electronic_reading_room/EFFR%20-%20FOIA.pdf (describing the policy by which the NSA should hand off information to the FBI as part of the minimization procedure).

215. Letter from Alexander W. Joel, Civil Liberties Prot. Officer, Office of the Dir. of Nat’l Intelligence, to Silvestre Reyes & Peter Hoekstra, Representatives, U.S. House of Representatives 6 (Sept. 17, 2007), available at <http://www.fas.org/irp/news/2007/09/joel091707.pdf>.

216. *Id.*

217. *Id.*

218. *Id.*

office, internal oversight of minimization is provided by the National Security Division at DOJ and the Office of General Counsel at ODNI.²¹⁹

In its PAA minimization procedures, discussed by NSA in answering questions from the Intelligence Committees and released following a FOIA request, NSA acknowledged that minimization is “not an exact science,” and yet “analysts over time develop an excellent working knowledge of their targets,” thus making mistakes in collecting foreign intelligence less likely.²²⁰ Reading between the redactions in the declassified answers, it is impossible to obtain a clear picture of minimization practice. NSA does object to codifying minimization procedures “because it can be difficult to change a statute if the procedures need to be changed in order to meet operational needs,” and it notes that NSA “has established extensive compliance mechanisms” to meet PAA requirements, all of which are subject to oversight and review by the NSA SIGINT Directorate Office of Oversight and Compliance, the Office of Inspector General, and the Office of General Counsel, in addition to the ODNI and DOJ.²²¹ While the limited transparency afforded by the ODNI letter and NSA procedures and responses to the Intelligence Committees’ questions promises continuing oversight, these documents do not provide substantive administrative safeguards, much less legislative standards, which would more effectively protect civil liberties following programmatic surveillance.

The most facile means for minimization prior to dissemination pursuant to FISA has been simply to redact U.S. person names and identifiers.²²² In the few settings prior to the FAA where the Attorney General could authorize surveillance without advance FISC approval, there had to be “no substantial likelihood” that the acquisition would reach “the contents of any communication to which a United States person is a party.”²²³ Because Congress recognized that U.S. person-communications collection could nonetheless occur in those situations, minimization required that none of the contents of such a communication could be disseminated “for any purpose or retained for longer than 72 hours” without a court order or an Attorney General determination that the information “indicates a threat of death or serious bodily harm to any person.”²²⁴ Although these steps were contemplated for surveillance undertaken without *any* prior FISC involvement, the limited role that the court plays in approving programmatic surveillance suggests that requiring a

219. *Id.* at 7–8.

220. NSA’s Minimization Procedures, in FOIA REQUEST BY ELECTRONIC FRONTIER FOUNDATION 000301 (Dec. 10, 2007), available at http://www.dni.gov/electronic_reading_room/EFFR%20-%20FOIA.pdf.

221. *Id.* at 000301, 000304.

222. KRIS & WILSON, *supra* note 192, at 9–27; cf. 50 U.S.C. § 1801(h)(2) (2006) (defining “minimization procedures” as those procedures protecting U.S. person identities).

223. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(a)(1)(B), 92 Stat. 1783, 1787 (codified at 50 U.S.C. § 1802(a)(1)(B) (2006)).

224. FISA § 101.

court order for dissemination of information about U.S. persons within days of collection through programmatic surveillance may serve the minimization objectives.

In its third report on improving information sharing,²²⁵ a Markle Foundation Task Force recommended responding to the problems of sharing too much or too little information with a government-wide authorized-use standard that “would improve the access, sharing, use, and protection of relevant information legally in the government’s possession while protecting privacy and civil liberties.”²²⁶ In addition to recommending the use of anonymization technology to enable information analysis without disclosure of personal identifying information, the Task Force recognized the need to balance potentially competing goals to account for the sensitivities of U.S. persons, while permitting information sharing to occur in a timely fashion.²²⁷ For information collected that is not about U.S. persons or is not personally identifiable, authorized use could be automatically generated by the digitized system.²²⁸

For such personal information about U.S. persons as is included in information proposed for use or dissemination, the requester would be required to “articulate a more specific authorized use to access that information . . . to meet a higher standard of care and need.”²²⁹ In other words, permission to use the information would be based on the nature and timing of the threat or mission at issue in an investigation. The authorized-use system would be set up so that “the more sensitive the information, the higher the required authorized use, the stricter the audit, and potentially, the greater the need for an official to consider approval for deanonymization.”²³⁰ Under authorized use, auditable records would be maintained for each dissemination, and audits and other forms of monitoring would be utilized to ensure enforcement of authorized use.²³¹

New legislation would prescribe the framework for an authorized-use system, and the Executive Branch would develop agency-specific guidelines or regulations to implement authorized use subject to the agency requirements and to specific legal authorities that apply to the agency’s processes.²³² The process for creating the guidelines or regulations should be as transparent as possible and it should include privacy and civil liberties officers from

225. MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT (2006).

226. *Id.* at 33.

227. *Id.* at 35–36.

228. *Id.* at 35.

229. *Id.*

230. *Id.* at 36.

231. *Id.* at 40. The Task Force also proposed that authorized use include a safe-harbor mechanism that would prohibit punitive action against any user of the system that used collected information following authorized-use guidelines. *Id.* at 40–41.

232. *Id.* at 34–35, 39.

the agencies, review by the Privacy and Civil Liberties Oversight Board, and then final approval by the President.²³³ For programmatic FISA surveillance, the guidelines should formalize standards of care and need for the retention and use of U.S. person information inadvertently collected, and they should require FISC approval of the guidelines and of dissemination decisions where personally identifiable information about individual U.S. persons would be transferred. Anonymization of U.S. person information should be required wherever possible, consistent with lawful surveillance objectives. The guidelines should also specify audit procedures, and the procedures and audit reports should be reported to Congress.

VI. Conclusion

When I first became a student of FISA, more than twenty years ago, I struggled to understand when a friend who worked inside the FISA process told me that we should worry less about what is collected and how and more about how what is collected is used. Eventually I learned about the importance of the now-lowered wall that separated foreign intelligence from law enforcement and about how minimization could protect private information.

Meanwhile the digital revolution and our data-driven society resulted in private industry having access to personal identifying information about most Americans. The constitutional and statutory law grew up around the premise that our voluntary sharing of that personal information with our credit card companies, ISPs, and banks eliminated any reasonable expectation of privacy in that information. When the government more prominently and aggressively began collecting and then mining that stream of data, especially after September 11, only a few limits were set on its use. Yet, when the TSP was exposed based on the same techniques, there was widespread condemnation of the Bush Administration. Why?

Part of the reason is that Americans did not know that the government could be listening in on or viewing their international telecommunications traffic, incoming and outgoing, and we feared that our conversations and e-mails were being monitored by someone at NSA. Once we learned more about the program, we also feared that officials were continuing to monitor our communications without probable cause and without the approval of any judge.

As we learned more about TSP and its follow-on iterations, as authorized by the FISC and then Congress, it became clear that the more significant privacy intrusion occurs not at the initial stage of flagging our calls or e-mails, but at the point when someone, looking at aggregate data for patterns or suspicious activity, decides to personally review an individual's communications. In other words, we should be worried more about what the data is used for, not so much that it is collected.

233. *Id.* at 39.

Although information sharing has been a mantra in recent years, and curtailing the uses of collected data cuts against sharing, important reasons exist for imposing controls in the newest FISA program. Data mining is more than the “automation of traditional investigative skills.”²³⁴ The “automation” may have a greater impact on personal privacy because the mass of data mined will generate more false positives than traditional police work, and, absent controls, the data may be preserved indefinitely for any use, including human review. To defend data mining by arguing, as Judge Richard Posner has, that “[c]omputer searches do not invade privacy because search programs are not sentient beings”²³⁵ is to ignore what happens to the data after it is mined.

Judge Posner concedes that programmatic surveillance produces many false positives But . . . the cost of false positives must be balanced against that of false negatives. . . . The intelligence services have no alternative to casting a wide net with a fine mesh if they are to have reasonable prospects of obtaining the clues that will enable future terrorist attacks on the United States to be prevented.²³⁶

If we accept the utility and inevitability of programmatic collection, it does not undermine collection to insist on targeting criteria that focus on the nature of the information sought and fulsome protections against retaining and disseminating collected personal information.

234. Taipale & Carafano, *supra* note 6, at 21.

235. Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 254.

236. *Id.* at 252–53.