National Security Law Journal

Excerpt from Vol. 4, Issue 1 (Fall/Winter 2015)

Cite as:

Patrick Walsh, *Planning for Change: Building a Framework to Predict Future Changes to the Foreign Intelligence Surveillance Act*, 4 NAT'L SEC. L.J. 1 (2015).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

PLANNING FOR CHANGE:
BUILDING A FRAMEWORK TO PREDICT FUTURE CHANGES TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Patrick Walsh*

In the last several years, the United States has begun to scrutinize the expansive surveillance powers that were enacted after September 11, 2001. Intelligence surveillance programs previously considered lawful and reliable ways to gather information are being rescinded by Congress, declared unlawful by the courts and restricted by the executive branch. In an era of increasing scrutiny on the intelligence community, national security professionals must look beyond the statutory authorization for intelligence gathering, and evaluate each intelligence program to determine if it will endure past current efforts to restrict government surveillance powers. This article will develop a framework to analyze our current intelligence gathering programs and determine which programs are at risk of removal by future executive, legislative or judicial action.

By examining the historical struggle between the intelligence community's need for broad powers to protect the nation from foreign enemies and our nation's strong commitment to protecting the civil liberties of citizens from government intrusion, a national security lawyer can determine how our nation has expanded, modified, restricted, and rescinded other intelligence gathering programs to meet the nation's national security goals. Comparing

* Associate Professor, International and Operational Law Department, The Judge Advocate General's School, United States Army, Charlottesville, Virginia. J.D., 1998, University of California at Berkeley; L.L.M., 2009, The Judge Advocate General's School, United States Army, Charlottesville, Virginia; L.L.M. (candidate) 2016, University of Virginia Law School. The author is a military reservist currently serving on active duty. In his civilian life, he is an Assistant United States Attorney who handles national security cases for the U.S. Attorney's Office in the District of Nevada.

the history and development with a modern look at how the public and the government have responded to current surveillance powers will illustrate the factors that create an increased risk for an intelligence program to be weakened or eliminated by judicial, legislative, or executive action. Using this framework, a cautious national security professional can carefully decide which of the currently available intelligence collection options are likely to both meet the current collection requirements and also endure the current increased scrutiny on surveillance. The Foreign Intelligence Surveillance Act ("FISA") will change again, and national security professionals must be prepared for these changes.

INTRODUCTION

The foreign intelligence surveillance framework has been modified significantly since the terrorist attacks of September 11,

2001.[1] Expansive surveillance powers were granted to the intelligence and law enforcement communities in order to protect the nation from future attacks.[2] A decade later, the validity of these same programs is being reexamined.[3] Foreign intelligence surveillance programs that were once considered lawful and reliable ways to gather information are being rescinded by Congress, declared unlawful by the courts, and restricted by the executive branch.[4] As a result, national security professionals in charge of gathering intelligence information and using it to protect the nation must reassess the information they have gathered and determine what to do with it. Officials wishing to use the intelligence as evidence in a criminal case must determine whether it is still admissible, even if the methods were lawful when the government first acquired the intelligence.[5] In addition to these considerations for gathering intelligence and prosecuting individuals, the intelligence community must reevaluate all of the remaining intelligence gathering programs to determine which programs Congress or the judiciary are more likely to remove, and which programs will remain available for future use.

In an era of increasing scrutiny on the intelligence community, national security professionals must look beyond the

---

[1] *See, e.g.*, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463, 2473 (2008).

[2] 50 U.S.C. § 1804(a)(6)(B); 122 Stat. at 2473.

[3] *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 810 (2d Cir. 2015) (holding that the Section 215 Program did not preclude judicial review); United States v. Mohamud, No. 3:10–CR–00475–KI–1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 86–97 (2014), https://www.pclob.gov/library/702-Report.pdf (detailing the PCLOB's review of the Fourth Amendment issues raised by the surveillance program operated under Section 702).

[4] *See* Memorandum from Jamie S. Gorelick, Deputy Att'y Gen., to Mary Jo White, U.S. Att'y, S. Dist. N.Y. et al. 1, https://fas.org/irp/ agency/doj/1995_wall.pdf [hereinafter Gorelick Memo]; *see also* Memorandum from Janet Reno, Att'y Gen., to Assistant Att'y Gen. et al. § (A)(6) (July 19, 1995), http:// www.fas.org/irp/agency/ doj/fisa/1995procs.html [hereinafter Reno Memo].

[5] *See Clapper*, 785 F.3d at 813; Issuance of Order, 50 U.S.C. § 1805 (2012).

statutory authorization for intelligence gathering and evaluate each intelligence program for the likelihood that the Court will revoke it, Congress will rescind it, or the executive branch will restrict it. This article will discuss an approach to scrutinize our current intelligence gathering and determine which programs are at risk to be removed by future executive, legislative, or judicial action.

This article begins its analysis in Part I, with an examination of the historical struggle between the intelligence community's need for broad powers to protect the nation from foreign enemies, and our nation's strong commitment to protecting the civil liberties of citizens from government intrusion. Understanding the development of this debate, which led to the Foreign Intelligence Surveillance Act ("FISA"),[6] gives context to how our nation has expanded, modified, restricted, and rescinded other intelligence gathering programs to meet the nation's national security goals. Intelligence professionals who are familiar with the genesis of the current intelligence gathering systems will be more adept at assessing which programs may disappear. Next, Part II will introduce FISA, and provide a brief explanation of how it works, and how it restricted sharing between the intelligence and law enforcement communities before the September 11, 2001, attacks. Part III examines the amendments to FISA after the September 11th attacks that expanded the ability to gather foreign intelligence and removed barriers to information sharing. It concludes with a look at how the public and the government have responded to these new expansive surveillance powers. Finally, Part IV analyzes the factors that create an increased risk for an intelligence program to be weakened or eliminated by judicial, legislative, or executive action.

I. THE BEGINNING OF THE INTELLIGENCE DEBATE—LIFE BEFORE FISA

The first decades of telephone wiretaps were without controversy, and the President conducted intelligence collection

[6] An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

without the involvement of other branches of government.[7] Telephone wiretaps during World War II were a prime example of national security intelligence collection without judicial approval.[8] Successive presidents expanded the use of these warrantless wiretaps to obtain national security and foreign intelligence information.[9] This policy continued until the 1960s with little concern or controversy from the legislative or judicial branches of government. However, that changed in the late 1960s when prosecutors attempted to use these wiretaps as evidence in criminal trials.[10]

*A. Pre-*Katz *Intelligence Gathering*

Prior to 1967, there was tacit judicial approval of all warrantless telephone surveillance.[11] In its 1927 decision in *Olmstead v. United States*, the Supreme Court held that telephone surveillance did not violate the Fourth Amendment because it did not constitute the requisite physical trespass.[12] Although this created the possibility of unrestrained government telephone surveillance, the executive and legislative branches later reduced that risk by prohibiting the use of wiretaps as evidence in court proceedings.[13] This created a civil liberties "compromise" where government agents

---

[7] Zweibon v. Mitchell, 516 F.2d 594, 674 (D.C. Cir. 1975) (Appendix A: Memorandum from President Franklin D. Roosevelt to Attorney General Robert Jackson); *see also* Herbert Brownell, Jr., *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 197-98 (1954).

[8] *Zweibon*, 516 F.2d at 674; *see also* Brownell, *supra* note 7, at 199-200.

[9] Memorandum from Att'y Gen. Herbert Brownell for J. Edgar Hoover, FBI Dir. 296-97 (May 20, 1954), *reprinted in* FRANK CHURCH ET AL., INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK 2, S. REP. NO. 94-755, at 296-97 (1976), http://www.intelligence.senate.gov/sites/default/files/94755_III.pdf; Memorandum from Att'y Gen. Nicholas Katzenbach for J. Edgar Hoover, FBI Dir. (Sept. 27, 1965), *reprinted in* S. REP. NO. 94-755, at 287; Press Release, U.S. Dep't of Justice (Sept. 12, 1973), *reprinted in* L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343, 1383 (2013).

[10] Katz v. United States, 389 U.S. 347, 353 (1967).

[11] Olmstead v. United States, 277 U.S. 438, 468-69 (1928).

[12] *Id.* at 466 (holding that there was no reasonable expectation of privacy because the bug was placed on the wire in a public area).

[13] *See* Nardone v. United States, 302 U.S. 379, 381 (1937); *see also* Radio Act of 1927, Pub. L. No. 632, § 27, 44 Stat. 1162, 1172 (1927); *see also* Department of Justice Appropriations Act of March 1, 1933, Pub. L. No. 387, 47 Stat. 1371, 1381 (1933).

had few limitations on their ability to use wiretaps, but little incentive to do so for anything other than to gather foreign intelligence.[14] Some began to see this compromise as a "national security exception" to the Fourth Amendment's warrant requirement—which permitted the use of national security wiretaps without a warrant, but prohibited the government from introducing any of this intelligence at trial.[15]

B. Katz *and Search Warrants for Wiretaps*

The Supreme Court again reviewed the lawfulness of warrantless wiretapping in *Katz v. United States*. Decided in 1967, *Katz* brought wiretaps under the protection of the Fourth Amendment while leaving open the possibility that certain circumstances could allow for national security wiretaps without a search warrant.[16] In *Katz*, the Supreme Court determined that Federal Bureau of Investigation ("FBI") Agents violated the Fourth Amendment when they obtained a telephone wiretap without first seeking a judicially authorized warrant.[17] Even though the wiretap did not involve a trespass, the Court held that it nonetheless constituted a Fourth Amendment "search" and was unconstitutional unless the agents obtained a judicially authorized search warrant to conduct the wiretap.[18] The Court further held that searches without judicially authorized search warrants "are per se unreasonable under the Fourth Amendment."[19] Courts have routinely followed the

[14] *Nardone*, 302 U.S. at 381. If it was inadmissible in court, it would not be useful in criminal investigations. Therefore, it would be primarily used only by those who gathered information for its intelligence value.
[15] *Katz*, 389 U.S. at 358 n.23; *see* Atkinson, *supra* note 9, at 1356 (explaining the detailed history of the origins and limits of the national security exception).
[16] *Katz*, 389 U.S. at 353 (reversing *Olmstead*).
[17] *Id.*
[18] *Id.* The Supreme Court overruled its prior decision in *Olmstead* when it determined that the Fourth Amendment can be violated without a physical trespass. *Id.*
[19] *Id.* at 357.

principle that searches without warrants carry a presumption of unreasonableness unless they fit into a narrow group of exceptions.[20]

Katz involved a wiretap for a criminal investigation into illegal gambling with no national security implications.[21] Nonetheless, the Court addressed national security wiretaps through dicta in its well-known footnote 23.[22] This footnote specifically raised the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security,"[23] but did not provide an answer, as the "question was not presented by this case."[24] Footnote 23 suggested the possibility that agents could conduct national security and foreign intelligence searches without obtaining a search warrant.[25]

Katz left a ray of hope for national security cases.[26] *Katz* was a criminal case with no national security or intelligence nexus, and the Court left open the possibility that agents could conduct national security and foreign intelligence searches without obtaining a search

[20] *Id.*; *see, e.g.*, Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (police may conduct an investigation if delay in obtaining a warrant would gravely endanger their lives or the lives of others); Cooper v. California, 386 U.S. 58, 87 (1967) (warrantless search of a seized automobile is proper if the search is directly related to why defendant was arrested); Brinegar v. United States, 338 U.S. 160, 174-77 (1949) (searches and seizures resulting from a police mistake may be permissible without a warrant if the mistake is reasonable); McDonald v. United States, 335 U.S. 451, 454-56 (1948) (police may conduct a search without a warrant when there are exigent or emergent circumstances, but inconvenience to the police officers and delay in preparing a warrant are not compelling reasons to justify a search without a warrant); Carroll v. United States, 267 U.S. 132, 153, 156 (1925) (police may search an automobile without a warrant if they have probable cause to believe evidence is located in the automobile).

[21] *Katz*, 389 U.S. at 354.

[22] *Id.* at 358 n.23 (planting the seed for the modern national security exception to the Fourth Amendment's warrant requirement thus becoming a well-known footnote (or exception?) in the national security arena).

[23] *Id.*

[24] *Id.*; *see* Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 273–74 (2009).

[25] *Katz*, 389 U.S. at 358 n.23.

[26] *Id.*; *see* Blum, *supra* note 24, at 273-74.

warrant.[27] The Court's language implicitly invited Congress to create a legislative framework for the application and approval of criminal wiretaps.[28] Because *Katz* did not explicitly hold on national security and foreign searches, law enforcement who sought to turn foreign intelligence into evidence for use in criminal prosecutions were left unsure whether their national security wiretaps obtained without a search warrant were lawful.

C. *Legislative Response to* Katz*, and Lead Up to FISA*

Congress responded to the Court's holding through the enactment of a broad framework for criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as "Title III").[29] However, Title III addressed only criminal wiretaps and left open the possibility that intelligence searches did not require a Title III judicially authorized warrant.[30] In vague language, Congress suggested that the President might have constitutional power to authorize intelligence searches without seeking judicial approval for cases involving national security.[31] Congress stated that Title III was not intended to "limit the constitutional power of the President . . . to protect the Nation against actual or potential attack,"[32] or "to obtain foreign intelligence information"[33] or "to protect the United States against any clear and present danger to the structure or existence of the Government."[34] One could also read this language much more narrowly however, to suggest that Congress did not agree that the President had such authority but was not trying to resolve that issue in this legislation.[35]

---

[27] *Katz*, 389 U.S. at 358 n.23.
[28] *Id.* (suggesting Congress could create "safeguards other than prior authorization by a magistrate" that could "satisfy the Fourth Amendment in a situation involving the national security").
[29] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197 (1968).
[30] *Id.* at §801(c); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. I, at § 101(b)(3).
[31] Pub. L. No. 90-351, tit. I, at § 101(b)(3).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *See id.*; *see also* Atkinson, *supra* note 9, at 1397.

The executive branch took the former, more expansive view, and continued to conduct national security wiretaps without judicial oversight or approval.[36]

The issue was brought to the Court's attention four years later, with a case involving the bombing of a Central Intelligence Agency Office in Ann Arbor, Michigan.[37] In *United States v. United States District Court* (now called the *Keith* case), the Supreme Court found that a warrantless national security wiretap conducted inside the United States violated the Fourth Amendment.[38] The fact that it was labeled a national security case did not make the warrantless surveillance lawful.[39] Once again, the Supreme Court did not clarify the scope of its decision to require warrants in national security cases.[40] The Court clearly held that search warrants are required for domestic national security cases.[41] However, the Court left open the possibility that warrantless wiretaps for extraterritorial national security cases may be lawful.[42]

Keith marked the beginning of increased concern and growing restrictions on the ability of intelligence professionals to collect and share national security information. But the executive branch did not heed the concerns expressed in *Keith*, and continued to gather intelligence information (or more precisely, information

[36] *See* Atkinson, *supra* note 9, at 1397 (the executive branch continued to authorize wiretaps without a warrant for national security purposes).
[37] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 299 (1972) (known as the *Keith* case after Judge Keith, who wrote the lower court opinion); *see* Atkinson, *supra* note 9, at 1381 (detailing the history of the origins and limits of the national security exception). Others have referred to this more generally as a "special needs" exception. *See* Owen Fiss, *Even in a Time of Terror*, 31 YALE L. AND POL'Y REV. 1, 25–27 (2012). This paper uses the phrase national security exception because it is more specific to the present topic.
[38] *Keith*, 407 U.S. at 299-300, 318.
[39] *Id.*
[40] *Id.* at 324.
[41] *Id.* The Court softened its holding by limiting the warrant requirement to the facts of this case, and also invited Congress to propose "reasonable standards" that may apply in domestic national security searches. *Id.*
[42] *Id.* at 323-24.

claimed to be for intelligence) without obtaining a search warrant.[43] Congress took notice of the executive's warrantless wiretapping and began to view the efforts to gather intelligence as overreaching and abusive.[44] As a result, Congress acted to investigate and eventually curb these perceived executive branch abuses of intelligence tools.[45]

II. FISA—THE BUILDING OF A WALL

The Watergate scandal brought the concern of misuse of the intelligence apparatus by the executive branch to the forefront of the national consciousness.[46] The United States Senate responded by setting up the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the Church Committee.[47] The Church Committee conducted many public hearings and published a detailed report citing numerous abuses of the executive branch, including cloaking warrantless surveillance of political dissidents and opponents under the guise of "national security."[48] These misdeeds extended to both the military and FBI, and they occurred in the Nixon administration as well as previous administrations.[49] To fix these abuses, Congress sought to create a comprehensive statutory framework requiring the executive branch to regulate intelligence collection within the United States.[50]

---

[43] *See* Charles R. Nesson, *Aspects of the Executive's Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps*, 49 IND. L.J. 399, 412-13 (1974).

[44] Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1255 (2003); *see also* FRANK CHURCH ET AL., INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK 2, S. REP. NO. 94-755, at 2-3 (1976).

[45] *See* CHURCH ET AL., *supra* note 44, at 2-3.

[46] *See* O'Connor & Rumann, *supra* note 43, at 1255.

[47] *See* CHURCH ET AL., *supra* note 44, at 4-5; *see generally* O'Connor & Rumann, *supra* note 44, at 1255.

[48] *See* Evan Tsen Lee, *The Legality of the NSA Wiretapping Program*, 12 TEX. J.C.L. & C.R. 1, 38-39 n.142 (2006).

[49] *Id.* at 38; *see also* Michael German, *Trying Enemy Combatants in Civilian Courts*, 75 GEO. WASH. L. REV. 1421, 1432 (2007).

[50] 50 U.S.C. § 1802 (1978).

Congress passed FISA in 1978, in part as a response to government abuses of wiretaps and in part as an answer to the invitation of the *Keith* court to address the issue of national security wiretaps.[51] FISA served as a comprehensive statutory framework for the executive branch to obtain judicially sanctioned wiretaps, gather foreign intelligence, and provide for national security.[52] The statute made Congress's intent clear, that wiretaps for intelligence purposes required judicial authorization through the newly created Foreign Intelligence Surveillance Court ("FISC").[53] After *Katz*, Title III, *Keith* and FISA, there were clearly defined limits on the ability of the intelligence community to gather intelligence information, particularly domestic intelligence information.[54] Both Congress and the public remained concerned of abuses and government officials in all three branches began to restrict not just the ability to obtain intelligence information, but also the ability to share the information collected. These restrictions were designed to limit the sharing of intelligence information with law enforcement personnel.

A. How FISA Worked and How it Restricted Sharing

FISA created an alternate path for the government to obtain wiretaps and search warrants in foreign intelligence cases.[55] For intelligence professionals, FISA had advantages over Title III criminal wiretaps; the court operated in a classified setting, interceptions could last for a longer duration, and the monitoring procedures were more advantageous to the government.[56] These

---

[51] *See* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1211, 1227 (2007).

[52] 50. U.S.C. § 1802. A detailed explanation of judicially authorized wiretaps under FISA is beyond the scope of this article, which will focus on the wiretaps conducted without a judicial warrant.

[53] *See* 50 U.S.C. §§ 1803, 1809(a)(1) (1978) (making it a crime to "engage in electronic surveillance . . . except as authorized by this Act."). A detailed explanation of judicially authorized wiretaps under FISA is beyond the scope of this article, which will focus on the wiretaps conducted without a judicial warrant.

[54] Katz v. United States, 389 U.S. 347, 358 n.23 (1967); United States v. U.S. District Court (*Keith*), 407 U.S. 297, 324 (1972); 50 U.S.C. § 1801(f) (2015).

[55] *See*, *e.g.*, 50 U.S.C. §§ 1802-1805 (2015) (detailing the process for the government to apply and get approved for electronic surveillance).

[56] *See* 50 U.S.C. §§ 1801(h), 1802(a) (2015 & 2010).

advantages raised the concern that the executive branch would use FISA as a way to circumvent the criminal court process in cases not involving foreign intelligence. Therefore, Congress wrote protections into the statute to ensure the government could only use the surveillance tools in FISA for gathering foreign intelligence.[57]

The statute required that "the purpose" of surveillance was to obtain "foreign intelligence information."[58] However, this language was subject to multiple reasonable interpretations.[59] What if the government wanted to obtain foreign intelligence information but also wanted to investigate a crime? Congress did not state whether "the purpose" meant the *only* pupose, the primary purpose or a significant purpose. The courts were left to resolve what "the purpose" means when the government is gathering foreign intelligence.[60]

Federal courts answered this question and took a very restrictive view of "the purpose" of FISA.[61] Every court to review the issue determined that "purpose" really meant "the *primary* purpose."[62] These courts reasoned that national security professionals seeking FISA authorization to wiretap an individual's

[57] 50 U.S.C. § 1804(a)(6)(B) (2010).
[58] *Id.* *See also* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS, 2D, §10.3 Westlaw (database updated July 2015).
[59] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 911 (4th Cir. 1980) (interpreting pre-FISA law and significantly influencing all subsequent cases); *In re* Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002) (discussing the development of the primary purpose test).
[60] 50 U.S.C. § 1804(a)(6)(B). *See also* KRIS & WILSON, *supra* note 58, at § 10.3.
[61] *See* KRIS & WILSON, *supra* note 58, at § 10.3; s*ee Truong Dinh Hung*, 629 F.2d at 915-16; *see also In re Sealed Case*, 310 F.3d at 725 (FISA Ct. Rev. 2002).
[62] *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *overruled by* United States v. Abu-Jihaad, 630 F.3d 102, 126 (2d Cir. 2010) (overruling court still acknowledging the "primary purpose" of FISA to collect foreign intelligence); United States v. Pelton, 835 F.2d 1067, 1074-75 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

phone must establish that the primary purpose of the investigation is to gather foreign intelligence.[63]

The primary purpose test still left theoretical room for law enforcement officers to participate in intelligence investigations. As long as foreign intelligence gathering was the *primary* purpose, there could potentially be *secondary* purposes.[64] One of those secondary purposes could be law enforcement, but involving law enforcement in the investigation creates risk. A reviewing court might disagree and decide—after the fact—the primary purpose was really law enforcement and not foreign intelligence.[65] Alternatively, a reviewing court may agree that the primary purpose was *initially* to gather foreign intelligence, but during the course of the investigation, the primary purpose switched to a law enforcement purpose.[66] This can happen when investigators begin to determine that prosecution is warranted and continue to use FISA approved surveillance while developing a criminal case.

The risk that a court may disapprove of the "purpose" of the investigation raised concerns in the Department of Justice ("DOJ"). Although Federal courts assumed that the sharing of FISA derived information after the investigation ended was permissible, government lawyers added additional executive branch restrictions to mitigate this risk.[67] A cautious executive branch, perhaps

[63] *See Truong Dinh Hung*, 629 F.2d at 915-16; *In re Sealed Case*, 310 F.3d at 725. *See also Johnson*, 952 F.2d at 572; *Pelton*, 835 F.2d at 1074-75; *Badia*, 827 F.2d at 1464; *Duggan*, 743 F.2d at 77.

[64] Courts before September 11, 2001 had found that the foreign intelligence exception applied where the "primary purpose" was the gathering of foreign intelligence. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Megahey, 553 F. Supp. 1180, 1189-90 (E.D.N.Y.1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984). *In re Directives* expanded the exception (for FISC purposes) to allow warrantless searches that met the lower "significant purpose" standard. *In re* Directives, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

[65] *See In re Sealed Case*, 310 F.3d at 725-26.

[66] *See id.* at 725-27.

[67] *Id.*

chastened by the past abuses, placed additional policy restrictions on the sharing of intelligence information.[68]

B. The Department of Justice and Its Restrictions on Access to Foreign Intelligence Information

The DOJ attorneys created policy restrictions on the sharing of intelligence information with law enforcement. These restrictions alleviated some of the risk of post facto judicial review of the "primary purpose" of the investigation.[69] After examining the relevant judicial opinions and the approving statements of the Congressional committees that oversee FISA cases, the DOJ added additional regulations to ensure that all intelligence investigations complied with the primary purpose test.[70] These procedures—and their implementation—made it nearly impossible to share intelligence information with law enforcement officials.[71]

The intent of the procedures was to separate counterintelligence investigations from criminal investigations and to prevent any appearance that the federal government was using the intelligence tools for the primary purpose of furthering a criminal investigation.[72] These restrictions created what one court later called a "wall" to prevent the FBI intelligence officials from communicating with the Criminal Division regarding intelligence investigations.[73] These restrictions that limited sharing intelligence information with law enforcement were in effect on September 11, 2001, and may have contributed to the failure to identify and locate the 9/11 hijackers and, perhaps, stop the September 11 attacks.[74] After the

---

[68] *See* Gorelick Memo, *supra* note 4, at 2-4; *see also* Reno Memo, *supra* note 4, at § (A)(6).
[69] *See* SELECT COMM. ON INTELLIGENCE, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. Rep. No. 660-98, at 14 (1984).
[70] *Id.* at 15.
[71] NAT'L COMM. ON TERRORIST ATTACKS, THE 9/11 COMMISSION REPORT: FINAL REPORT ON THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 271 (2004) [hereinafter THE 9/11 COMMISSION REPORT].
[72] Gorelick Memo, *supra* note 4, at 2-3.
[73] *See In re* Sealed Case, 310 F.3d 717, 728 (2002).
[74] THE 9/11 COMMISSION REPORT, *supra* note 71, at 271-72, 277 (noting "deep institutional failings within the government" including (1) a decrease in FISA

September 11, 2001, attacks, Congress amended FISA to eliminate the restrictions imposed by the judicial and executive branches, and began to expand the tools available to the intelligence community to address the threat of terrorism.[75]

III. THE COUNTRY'S ABOUT-FACE: EMPOWERING LAW ENFORCEMENT TO USE FISA

After the attacks of September 11, 2001, the executive and legislative branches realized that the restrictions placed on the intelligence tools from 1968 to 2001 created a system ill fitted to protect the nation from contemporary threats.[76] Both Congress and the President took actions to remove these long-standing restrictions, and created new and broader tools to aid in the collection and sharing of intelligence with law enforcement. Some of these broad intelligence collection programs expanded authorities within FISA.[77]

A. Removing Restrictions and Adding New Authorities to FISA

Congress dismantled the wall that courts erected around the primary purpose requirement in FISA.[78] Courts had previously read into FISA a requirement that the "primary purpose" of FISA surveillance must be to gather foreign intelligence.[79] Congress eliminated this requirement by changing the text from "the purpose" to a "significant purpose."[80] Congress added the word "significant" to destroy the executive created wall, which had restricted the sharing of intelligence with law enforcement, and to encourage information

applications leading up to the attacks, (2) some of the FISA wiretaps were discontinued before September 11, 2001, and (3) there was a misunderstanding about the ability to share FISA information on one of the 9/11 hijackers that prevented investigators from taking action that "could have derailed" the 9/11 attacks).

[75] Pub. L. 261-261, 122 Stat. 2463, 2473 (2008).

[76] THE 9/11 COMMISSION REPORT, *supra* note 71, at 277.

[77] *See id.*; 122 Stat. at 2473.

[78] 50 U.S.C. § 1804(a)(6)(B) (2012).

[79] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[80] *See* 50 U.S.C. § 1804(a)(6)(B) (2012).

sharing.[81] Under the revised law, FISA tools could be used even if there was a law enforcement purpose to the investigation.[82] The intelligence community was now strongly encouraged to share relevant information with law enforcement.

Congress took additional steps to increase the gathering of foreign intelligence. From President Bush's warrantless Terrorist Surveillance Program to the FISA Amendments Act of 2008, Congress, and the executive branch eased restrictions on intelligence gathering to permit widespread information collecting and sharing.[83] Faced with the external threats from terrorist organizations, the executive, legislative, and judicial branches found a common purpose in approving greater communication between the intelligence and law enforcement communities.[84] However, the government made many of these expansions in secret or without significant public discussion.[85] As these programs became public, the public raised concerns about the expansive and intrusive intelligence tools given to law enforcement. The concerns raised about these new intelligence-gathering authorities mirrored those raised forty years before.

B. Rising Concerns of Misuse of the New FISA Programs

Although changes to FISA noted in Section A were debated and enacted in public, other intelligence gathering programs were created in secret.[86] These programs came to be through executive actions and expansive, but classified, interpretations of FISA by the

---

[81] 50 U.S.C. § 1804(a)(6)(B) (2006).
[82] 122 Stat. at 2473.
[83] *See* Jewel v. NSA, No. 08-cv-04373, ¶ 6 (N.D. Cal. Dec. 20, 2013). In 2007, Congress passed the Protect America Act, which expired in February 2008. Pub. L. No. 110-55, 121 Stat. 552 (2007); 122 Stat. at 2473.
[84] *See Jewel*, No. 08-cv-04373, at ¶ 6.
[85] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005) (discussing the leak of the secret Terrorist Surveillance Program), http://www.nytimes.com/2005/12/16/ politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0; Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (Jun. 11, 2013) (which exposed the leaked information on the bulk collection of metadata and other classified programs) http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
[86] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85.

FISC.[87] The world learned of these secret intelligence tools through leaks of classified information and authorized declassification by the executive branch.[88] The reaction to these intelligence tools caused a significant debate and calls for restrictions on intelligence gathering.[89]

On October 4, 2001, President George W. Bush secretly authorized the Terrorist Surveillance Program, permitting the National Security Agency ("NSA") to wiretap communications from members of Al Qaeda to individuals within the United States.[90] The President later claimed that he had executive authority, based in the Constitution itself, to conduct this action.[91] These wiretaps were conducted outside of the FISA process and without any judicial oversight or approval.[92]

Eventually, a leak and subsequent confirmation by the Executive made the Terrorist Surveillance Program public.[93] Many experts argued these wiretaps were illegal under FISA or another federal law.[94] One federal district court agreed, determining that the program violated the Constitution because it permitted searches without judicially authorized warrants.[95] Instead of appealing the decision, the executive branch sought Congressional approval for the program.

---

[87] *See* Public Declaration of James R. Clapper, Director of National Intelligence at 6, Jewel v. NSA, No. 07-cv-693-JSW (N.D. Cal. Dec. 20, 2013); *see In re* Application of the FBI for the Production of Tangible Things (2013) (No. BR 13-80, http://www.dni gov/files/documents/PrimaryOrder_ Collection_215.pdf [hereinafter *In re* Application of the FBI].

[88] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85.

[89] Serwer, Adam, *New calls for surveillance reform after Snowden,* MSNBC (September 25, 2013), http://www.msnbc.com/msnbc/new-calls-surveillancereform-after.

[90] Risen & Lichtblau, *supra* note 85; *see* Public Declaration of James R. Clapper, Director of National Intelligence, *supra* note 87, at 6.

[91] U. S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 5, 17 (2006), http://www. usdoj.gov/opa/whitepaperonnsalegal authorities.pdf.

[92] *Id.*

[93] Risen & Lichtblau, *supra* note 85.

[94] *Id.*

[95] ACLU v. NSA, 438 F. Supp. 2d 754, 775-82 (E.D. Mich. 2006).

C. *Responses to the Post-9/11 Expansion of Federal Investigatory Authority*

Congress eventually agreed to a modified version of the program and passed the FISA Amendment Act of 2008.[96] The legislative solution in response to the Terrorist Surveillance Program's warrantless wiretaps had its own potential drawbacks because it legislated an avenue for the government to obtain wiretaps *without* a judicially authorized search warrant.[97]

Section 702 of FISA Amendment Act permitted the executive branch to conduct warrantless wiretaps of foreign persons outside the United States to gather foreign intelligence.[98] The FISC has limited involvement; it merely approves the targeting and minimization procedures used generally by the intelligence community, but it does not approve individual surveillance.[99] In addition, the FISC does not approve any individual interception, nor does it determine that there is probable cause the interception will gather foreign intelligence information.[100]

Since the inception of Section 702 interceptions, there have been numerous mistakes, misuses, and abuses of the program.[101] Individual intelligence analysts have made improper queries without permission, have queried Section 702 databases accidentally, and have queried Section 702 databases for U.S. persons when they should have only queried foreign nationals.[102] There have also been

---

[96] In 2007, Congress passed the Protect America Act, which expired in February 2008. Pub. L. No. 110-55, 121 Stat. 552 (2007). The FISA Amendment Act was passed in 2008 and is still current law; Pub. L. No. 110-261, 122 Stat. 2463, 2473 (2008).

[97] 122 Stat. at 2473.

[98] Procedures for Targeting Certain Persons Outside the United States Other than United States Persons, 50 U.S.C. § 1881a(a) (2015).

[99] 50 U.S.C. § 1881a(a).

[100] *Id.*

[101] 158 CONG. REC. S8457 (daily ed. Dec. 28, 2012) (Statement of Sen. Feinstein).

[102] *See* U.S. DEP'T OF JUSTICE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 33 (2013), http://www. dni.gov/files/documents/ Semiannual%20 Assessment%20of%20Compliance%20with%20procedures%20 and% 20guide lines%20issued%20pursuant%20to%20Sect%20702%20of%2FISA.pdf.

systematic errors, where the collection system collects too much information because of technical errors without solutions.[103] In short, the government conceded that its collection process is flawed and a certain portion of its interceptions will be wholly domestic communications.[104] The government admitted that it could not conduct the program without a small portion of its activity being outside of its permissible interception. So far, no court has ruled that the Section 702 program is per se unlawful because of this problem, but this issue is just beginning to be reviewed in federal courts.

The Terrorist Surveillance Program and the enactment of Section 702 were not the only programs that permitted the warrantless collection of information. The disclosure of classified surveillance programs by Edward Snowden created significant public outcry.[105] Although the programs disclosed by Snowden dealt with the interception of "metadata" and not the content of communications, the collection of vast amounts of information on ordinary Americans caused a national uproar.[106] This program—approved by the FISC based on an expansive reading of a section of FISA relating to the search of business records—permitted the government to collect limited information on all Americans (a bulk collection), on the condition that it could not be searched unless the government had specific suspicion that it was connected to foreign intelligence.[107]

The program leaked by Snowden was approved by the FISC but it nonetheless raised concerns similar to those found during the

---

[103] *Id.* at 32.
[104] 50 U.S.C. § 1881a(a).
[105] Greenwald et al., *supra* note 85.
[106] *Id.*; *see also In re* Application of the FBI, *supra* note 87.
[107] *See* 50 U.S.C. § 1861 (2015) (commonly referred to as Section 215). *See* Office of the Dir. of Nat'l Intelligence Pub. Affairs Office, Newly Declassified Documents Regarding the Now-Discontinued NSA Bulk Electronic Communications Metadata Pursuant to Section 402 of the Foreign Intelligence Surveillance Act (Aug. 11, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1099-newly-declassified-documents-regarding-the-now-discontinued-nsa-bulk-electronic-communications-metadata-pursuant-to-section-401-of-the-foreign-intelligence-surveillance-act?highlight= WyJuZXdseSIsImRlY2xhc3 NpZmllZCIsIm5ld2x5IGRlY2xhc3NpZmllZCJd.

Church Committee 45 years earlier.[108] The public concern was that current oversight of the government's use of intelligence tools was insufficient to protect the liberties of everyday Americans.[109] Public perception once again shifted to the belief that the government was misusing these intelligence tools to spy domestically on Americans with little connection to national security.[110] The courts eventually weighed in, and the Second Circuit Court of Appeals ruled that this bulk collection program is inconsistent with the statutory language of FISA, and thus, is unlawful.[111] Any information gathered from the bulk collection program is now likely inadmissible in a criminal prosecution as the fruit of an illegal search.[112]

Congress responded to these concerns and eliminated the government's bulk collection of limited information on Americans, but it transferred this collection to private companies who are required to retain information they collect and have it available for search.[113] Only time will tell if this revision meets with the Court's interpretation of the statute and the Fourth Amendment to the Constitution, and if Congress and the Executive will remain satisfied that this revised provision achieves the appropriate balance between civil liberty and national security.

---

[108] CHURCH ET AL., *supra* note 44, at 5-6; Diane C. Piette & Jesselyn Radack, *Piercing the "Historical Mists:" The People and Events Behind the Passage of FISA and the Creation of the "Wall*," 17 STAN. L. & POL'Y REV. 437, 448 (2006).

[109]Greenwald et al., *supra* note 85.

[110] James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, THE GUARDIAN (Aug. 9, 2013), http://www.the guardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls; Laura K. Donohue, *NSA Surveillance May be Legal—but it's Unconstitutional*, THE WASH. POST (June 21, 2013), http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html.

[111] *Clapper*, 785 F.3d at 818-20.

[112] *See* 50 U.S.C. 1806(e) (2015) (providing that a defendant may move to suppress information that is unlawfully acquired).

[113] *See* Erin Kelly, *Senate Approves USA Freedom Act*, USA TODAY (June 2, 2015), http://www.usatoday.com/ story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/.

IV. PLANNING FOR CHANGE: WHAT INTELLIGENCE PROGRAMS ARE AT RISK TODAY

The debate over the Snowden-leaked program of bulk collection of information on Americans highlights the concern that national security professionals must face: how do they turn intelligence information into criminal evidence when they cannot be certain that current intelligence programs will be lawful at the time of trial? The program leaked by Edward Snowden was a statutory based collection program—FISA Section 215—reauthorized multiple times by the FISA Court before it was ultimately ruled unlawful.[114] If national security professionals cannot rely on judicial interpretations of statutory law to build cases, how can they continue to use the federal courts as a reliable solution to respond to current and future national security threats?

The answer involves risk analysis, something that is at the heart of intelligence analysis. When the legal climate is rapidly changing in the national security community, professionals must conduct a risk analysis of not only the threats to the nation, but also the risks that intelligence programs will become unavailable in the future, and render their evidence potentially inadmissible. A careful review of the past and present controversies around intelligence collection demonstrate three factors that national security professionals can use to evaluate the risk of losing intelligence tools and the information gathered from them. These factors are: (1) whether knowledge of the program is public or secret, (2) whether courts have approved the use of the program, and (3) whether the intelligence collection procedures resemble criminal evidence gathering procedures that courts are comfortable with allowing.

Turning to the first factor, classified sources and methods will eventually be made public—through leaks, declassification, or other means.[115] National security professionals must accept this as

---

[114] *See* In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted] (No. BR 15–24), at *3 (FISA Ct. Rev. Feb. 26, 2015); *see also Clapper*, 785 F.3d at 801-02, 820-22, 826 (finding the program was unlawful).

[115] *See, e.g.*, Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; David Kravets, *Declassified Documents Prove NSA is Tapping the Internet*, WIRED

fact. Each time one of the classified intelligence programs mentioned above was made public, there were negative consequences for both the intelligence program and the information gained from it.[116] The Terrorist Surveillance Program was leaked to the media and later confirmed by the President.[117] Subsequently, a district judge found the program to be unlawful.[118] Edward Snowden leaked the Section 215 bulk data collection program—and a federal appellate court found that the program was unlawful.[119] There is a lesson to be learned from this: intelligence gathering programs that the government keeps secret carry increased risk that they will be determined to be unlawful when the public finally learns about them.

The general public can learn about many intelligence programs through publicly available information like the statutes that authorize their use. The programs are public knowledge even though their use in a particular case is classified.[120] Traditional FISA warrants are a perfect example.[121] While the targets of FISA warrants are classified, the program itself is not. Both Congress and the courts recognize the program, the process to obtain warrants, and their use. These public intelligence programs carry less risk that they will be unavailable in the future.

MAGAZINE, Aug. 21, 2013, http://www.wired.com/2013/ 08/nsa-tapping-internet/ (declassified); John Diamond & David Jackson, *Surveillance Program Protects Country, Bush Says,* USA TODAY (Jan. 23, 2006), http://usatoday30.usatoday.com/ news/washington/2006-01-23-bush_x.htm (other means, like spontaneous Presidential confirmation).

[116] *See, e.g.*, Donohue, *supra* note 110; Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; *See* Julian Hattem, *Time for a New Church Committee? Ex-Staffers Think So*, THE HILL, Jan. 27, 2015, http://thehill.com/policy/technology/ 230822-time-for-a-new-church-committee-ex-staffers-think-so; Ball & Ackerman, *supra* note 102.

[117] Risen & Lichtblau, *supra* note 85; Greenwald et al., *supra* note 85; Diamond & Jackson, *supra* note 115.

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

[119] *Clapper*, 785 F.3d at 793.

[120] *See generally*, 50 U.S.C. §§ 1801-1805 (2015) (traditional FISA warrants for wiretaps); 50 U.S.C. § 1861 (2015) (permits collection of business records without bulk collection).

[121] 50 U.S.C. §§ 1801-1805.

The second factor pertains to the legal risk for classified programs. Intelligence programs that require court approval are more likely to endure than those done without judicial oversight. The more input a judicial officer had in approving the collection of information, the more likely a subsequent judge will permit the introduction of that information as evidence in court. The gathering of information under Executive Order 12333 and FISA Section 702 are examples of programs that have less judicial oversight.[122] This lack of judicial input during collection creates risk that a court overseeing the admission of that evidence in a criminal case will determine it is inadmissible. Programs that involve judicial officers in the process and obtain judicially sanctioned collection efforts are far more likely to be sustained in the future. The Section 215 bulk collection program may seem like an exception, but it actually proves the point.[123] The court ruled that the program violated the statute.[124] The bulk collection program is an example of an intelligence program that has risk of being lost because it was conducted in secret and without any corollary to a traditional criminal program.[125]

Third, the risk of having programs overturned is lower when using intelligence programs that have similarities to ordinary criminal investigative tools. When attempting to turn intelligence information into criminal evidence it helps to work with an intelligence program that has similar procedures to traditional criminal tools. Again, traditional FISA wiretaps are a good example. FISA wiretaps require an application to a judge, with a sworn affidavit, where a judge finds probable cause, and issues a limited warrant.[126] While the specific procedures and findings differ from a criminal Title III warrant, the similarities between the intelligence tool and the criminal tool make it more palpable to courts and juries to accept the evidence.[127] Using tools that have no corollary in the criminal system raises concerns that the information was obtained without following the normal checks on government conduct.

---

[122] *See* Exec. Order No. 12333, 46 F.R. 59941 (1981); 50 U.S.C. § 1802.
[123] 50 U.S.C. § 1861 (permits an order to produce certain business records).
[124] *See Clapper*, 785 F.3d at 826.
[125] *Id.*; 50 U.S.C. § 1861.
[126] *See* 50 U.S.C. § 1805.
[127] *Compare* 50 U.S.C. §§ 1801-1804 *with* Fed. R. Crim. P. 41.

Courts are more likely to question the tool's legality if it was not involved in the process to use the tool.

V. CONCLUSION

Our nation has only begun to evaluate what changes to make to the current intelligence programs. United States history demonstrates that Congress, the courts, and the executive branch will constantly struggle with the balance of giving national security professionals the tools needed to protect the nation from threats and giving our citizens the protections needed to secure their civil liberties. Intelligence professionals need to carefully examine the current use of intelligence programs because these programs, and how they can be used, will change. Some intelligence programs will be modified and restricted. Others will be removed by executive, legislative, or judicial action.

National security professionals who must transform intelligence into evidence in criminal cases must be especially wary. Courts may review intelligence programs in the future and retroactively determine they were unlawful. Any evidence law enforcement gathers pursuant to those programs may not be admissible when the national security case gets to trial. But a cautious national security professional can carefully decide which of the currently available intelligence collection options are likely to both meet the current collection requirement and also endure increased scrutiny so the information is useful in the future. Intelligence professionals excel at risk analysis; now they must use those skills to evaluate the durability of the collection programs available to them. FISA will change again, and national security professionals must be prepared for these changes.