Losing Tools in the Intelligence Toolbox: Predicting Future Changes to FISA to Protect Future National Security Prosecutions

Patrick Walsh, The U.S. Army Judge Advocate General's Legal Center and School

Available at: https://works.bepress.com/patrick-walsh/3/
Melvin Otey
Transnational Organized Crime

Al Saibini
Supply and Demand: Drug Smuggling in 2015

Patrick Walsh
Losing Tools in the Intelligence Toolbox: Predicting Future Changes to FISA to Protect Future National Security Prosecutions

Jerome M. Conley
The Intersection of Wildlife Trafficking and Insurgencies in Africa

Yangmo Ku
Engagement or Pressure? Dealing with North Korea’s Crimes against Humanity

Kristy Holtfreter and Travis J. Meyers
Challenges for Cybercrime Theory, Research, and Policy

Jennifer Brooke Marshall
A Case Study on Eurasian Organized Crime Groups Recently Indicted In New York
LOSING TOOLS IN THE INTELLIGENCE TOOLBOX:
PREDICTING FUTURE CHANGES TO FISA TO PROTECT FUTURE NATIONAL SECURITY PROSECUTIONS

Patrick Walsh
I. Introduction

National Security Professionals charged with protecting the country from harm must feel like an auto mechanic who can’t find his favorite wrench. Foreign intelligence surveillance tools that were once considered lawful and reliable ways to gather information are being rescinded by Congress, declared unlawful by the courts and restricted by the executive branch (U.S. Department of Justice, 1995). Any information gathered using these lost tools may not be admissible in a criminal case, even though the methods were considered lawful when the information was acquired (American Civil Liberties Union v. Clapper, 2015). How can those in the intelligence community determine which tools are at risk of being removed from the toolbox and which will be an enduring lawful means to build solid intelligence for the future?

In an era of increasing scrutiny on the intelligence community and its tools, national security professionals must look beyond the statutory authorization for intelligence gathering and evaluate each intelligence tool for the likelihood that it will be revoked by the court, rescinded by Congress or restricted by the executive branch. This article will discuss an approach to scrutinize our current intelligence gathering tools and determine which ones are at risk to be removed by future executive, legislative or judicial action. To do this, one must analyze the historical struggle between the intelligence community’s need for broad powers to protect our nation from foreign enemies and our nation’s strong commitment to protect our civil liberties from government intrusion. Understanding the development of this debate, which led to the Foreign Intelligence Surveillance Act, will give context to how our nation has expanded, modified, restricted and rescinded the various intelligence gathering tools to meet the nation’s national security goals. Intelligence professionals who know how we got to our current intelligence gathering tools will better be able to assess which tools may disappear.

II. The Beginning of the Intelligence Toolbox Debate—Life Before FISA

In the beginning, intelligence collection was conducted at the pleasure of the President without interference from the other branches of government (Zweibon v. Mitchell, 1975). President Franklin Delano Roosevelt is the first President known to rely on National Security wiretaps; he sanctioned telephone wiretaps for national security conducted without judicial warrants before and during World War II (Brownell, 1954). Successive presidents, following Roosevelt’s lead, expanded the use of these warrantless wiretaps to obtain national security and foreign intelligence information (U.S. Senate, 1976). There were far fewer wiretaps approved and there was little concern or controversy from the legislative or judicial branches of government during the 1940s, 50s and early 60s. But that changed in the late 1960s when intelligence wiretaps were being used as evidence in criminal trials (Katz v. United States, 1967).

The courts were the first to act to curb the use of national security wiretaps. In 1967, the United States Supreme Court reversed forty years of precedence and held that criminal telephone wiretaps were “searches” and unlawful without a search warrant (Katz v. United States, 1967). In Katz v. United States the Court determined that the Federal Bureau of Investigation violated the Fourth Amendment...
when they obtained a telephone wiretap without first seeking a judicially authorized warrant (Katz v. United States, 1967). Katz left a ray of hope for national security cases (Katz v. United States, 1967).

Katz was a criminal case with no national security or intelligence nexus, and the Court left open the possibility that agents can conduct national security and foreign intelligence searches without obtaining a search warrant (Katz v. United States, 1967). The Court invited Congress to create a legislative framework for the application and approval of criminal wiretaps (Katz v. United States, 1967). So law enforcement who sought to turn information gathered from intelligence tools into evidence at a criminal trial were left unsure whether their national security wiretaps obtained without a search warrant were lawful.

Congress enacted a broad framework for criminal wiretaps in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to now as “Title III”) (Title III, 1968). But Title III addressed only criminal wiretaps and left open the possibility that intelligence searches may be permitted without a need for a Title III judicially authorized warrant (Title III, 1968). In vague language Congress suggested that the President may have constitutional power to authorize intelligence searches without seeking judicial approval for cases involving national security (Title III, 1968).

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,” or “to obtain foreign intelligence information” or “to protect the United States against any clear and present danger to the structure or existence of the Government” (Title III, 1968). But this language could also be read much more narrowly to suggest that Congress did not agree that the President had such authority but was not trying to resolve that issue in this legislation (Atkinson, 2013). The executive branch took the former, more expansive view, and continued to conduct national security wiretaps without judicial oversight or approval (Atkinson, 2013).

The issue returned to the courts four years later, with a case involving the bombing of a Central Intelligence Agency Office in Ann Arbor, Michigan (United States v. U.S. District Court, 1972). 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 (United States v. U.S. District Court, 1972). The fact that it was labeled a “national security case” did not make the warrantless surveillance lawful (United States v. U.S. District Court, 1972). Once again, the Supreme Court left some doubt as to the scope of its decision to require warrants in national security cases (United States v. U.S. District Court, 1972). The Court clearly held that search warrants are required for domestic national security cases (United States v. U.S. District Court, 1972). But the Court left open the possibility that warrantless wiretaps for national security cases outside the United States may be lawful (United States v. U.S. District Court, 1972). The Court did not decide that issue, it left it for resolution in a future case (United States v. U.S. District Court, 1972).
Keith marked the beginning of increased concern and growing restrictions on the ability of intelligence professions 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 claimed to be for intelligence) without obtaining a search warrant (U.S. Dep’t of Justice, 1973). But Congress was beginning to take notice of the executive action and began to view the efforts to gather intelligence as overreaching and abusive (O’Connor & Rumann, 2003). So Congress acted to investigate and eventually curb these perceived executive branch misuse of intelligence tools (U.S. Senate, 1976).

III. The Foreign Intelligence Surveillance Act—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. 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 (U.S. Senate, 1976). 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” (Lee, 2006). These misdeeds extended to the military, the Federal Bureau of Investigation and occurred in both the Nixon administration and previous administrations (Lee, 2006). Congress decided to create a comprehensive statutory framework requiring the executive branch to regulate intelligence collection within the United States (50 U.S.C. § 1801, 1978).

Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) 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 (Banks, 2007). Congress created in FISA a comprehensive statutory framework for the executive branch to obtain judicially sanctioned wiretaps to gather foreign intelligence and provide for national security (50 U.S.C. § 1801, 1978). Congress clearly declared its view that wiretaps for intelligence purposes required judicial authorization through the newly created Foreign Intelligence Surveillance Court (FISC) (50 U.S.C. § 1801, 1978). 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 (Katz v. United States, 1967). But concerns of abuse were still prevalent, and a push began to restrict not just the ability to obtain intelligence information, but also to restrict the ability to share the information once it is collected by the government. These restrictions were designed to limit the sharing of intelligence information with law enforcement personnel.

IV. How FISA Worked and How it Restricted Sharing
The FISA created an alternate path for the government to obtain wiretaps and search warrants in foreign intelligence cases (50 U.S.C. § 1801, 1978). For intelligence professionals, FISA had advantages over Title III criminal wiretaps; the court was conducted in a classified setting, interceptions could last for a longer duration and the monitoring procedures were more advantageous to the government (50 U.S.C. §§ 1801(h) and 1802(a)). These advantages raised the concern that the executive branch would use the FISA as a way to circumvent the criminal court process in cases not involving...
foreign intelligence. Therefore, Congress wrote into the statute protections to ensure the FISA would be used only for the purpose of gathering foreign intelligence (50 U.S.C. § 1804(a)(7)(B)).

The statute required that “the purpose” of a surveillance was to obtain “foreign intelligence information” (Kris & Wilson, 2012, §10.3). But this language was subject to more than one interpretation (U.S. v. Truong Dinh Hung, 1980). What if the government wanted to obtain foreign intelligence information but also wanted to investigate a crime? The courts were left to resolve the meaning of the “the purpose” of the surveillance was to gather foreign intelligence (Kris & Wilson, 2012, §10.3).

Federal courts took a very restrictive view of “the purpose” of FISA (In re Sealed Case, 2002). Every court to review the issue determined that “purpose” really meant “the primary purpose” (In re Sealed Case, 2002). Put another way, the national security professionals seeking Foreign Intelligence Surveillance Court permission to wiretap an individual’s phone must establish that the primary purpose of the investigation is to gather foreign intelligence (U.S. v. Johnson, 1991).

The primary purpose test still left theoretical room for law enforcement in intelligence investigations. As long as foreign intelligence gathering was the primary purpose, there could potentially be secondary purposes. One of those secondary purposes could be law enforcement. But involving law enforcement in the investigation created risk; a reviewing court might disagree and decide—after the fact—the primary purpose was really law enforcement and not foreign intelligence (In re Sealed Case, 2002).

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 (In re Sealed Case, 2002). This can happen when investigators begin to determine that prosecution is warranted and continue to use FISA approved surveillance while developing a criminal case.

Federal courts assumed that the sharing of FISA derived information after the investigation ended was permissible (In re Sealed Case, 2002). But a cautious executive branch, perhaps chastened by the past abuses, placed additional policy restrictions on the sharing of intelligence information (U.S. Department of Justice, 1995).

C. The Department of Justice and Its Restrictions On Access to the Intelligence Toolbox

The Department of Justice attorneys created policy restrictions on the sharing of intelligence information with law enforcement as a way to manage the uncertainty of the after the fact judicial review of the “primary purpose” of the investigation (U.S. Senate, 1984). After reviewing the judicial opinions mentioned above and the approving statements of the Congressional committees that oversee FISA cases, the Department of Justice decided to add additional regulations to ensure that all intelligence investigations complied with the primary purpose test (U.S. Senate, 1984). These procedures—and their implementation—made it nearly impossible to share intelligence information with law enforcement officials (Kean & Hamilton, 2004).
The procedures were intended to separate the counterintelligence investigation from criminal investigations and to prevent any appearance that the intelligence tools were being used solely to further a criminal investigation (U.S. Department of Justice, 1995). 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 (In re Sealed Case, 2002). 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 stop the September 11 attacks (Kean & Hamilton, 2004). After the 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 (122 Stat. 2463, 2473, 2008).

V. The Country’s About-Face: Opening the FISA Toolbox to Everyone

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 the current threats (Kean & Hamilton, 2004). Both Congress and the President took actions to remove these long standing restrictions and create new and broader tools to aid in the collection of intelligence, the sharing of it with law enforcement and the protection of the nation from these threats (50 U.S.C. § 1804(a)(6)(B) (2006)). Some of these changes involved the FISA (122 Stat. 2463, 2473).

Congress dealt with the wall that was erected around the primary purpose requirement in FISA. Congress changed “the purpose” to a “significant purpose” with the intention of destroying this wall and encouraging information sharing between intelligence and law enforcement (50 U.S.C. § 1804(a)(6)(B) (2006)). Under the revised law, FISA tools could be used even if there was a law enforcement purpose to the investigation (122 Stat. 2463, 2473). The intelligence community was now strongly encouraged to share relevant information with law enforcement.

Further efforts were undertaken to increase the gathering of foreign intelligence. From President Bush’s warrantless Terrorist Surveillance Program to the FISA Amendments Act of 2008, restrictions on intelligence gathering were eased to permit widespread collecting and sharing of information (Public Declaration of James R. Clapper, 2007). Faced with the external threats from terrorist organizations, Congress, the executive branch and the courts found a common purpose in approving greater communication between the intelligence and law enforcement communities (Public Declaration of James R. Clapper, 2007). But many of these expansions were approved or conducted in secret or without significant public discussion. As these programs became public, the public raised concerns about the expansive and intrusive intelligence tools given to law enforcement. These concerns mirrored those raised forty years before.

VI. Rising Concerns of Misuse of the Intelligence Toolbox

Changes to FISA were debated and enacted in public, but other tools were passed in secret either by executive action or through expansive interpretations of FISA made in classified setting by the
Foreign Intelligence Surveillance Court (Risen & Lichblau, 2005). These secret intelligence tools were subsequently disclosed to the world either through leaks of classified information or through declassification by the executive branch. It is the reaction to these intelligence tools that is causing the greatest debate and calls for restrictions on intelligence gathering today.

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 (Risen & Lichblau, 2005). The President later claimed that he had executive authority, based in the Constitution itself, to conduct this action (U.S. Department of Justice, 2006). These wiretaps were conducted outside of the FISA process and without any judicial oversight or approval (U.S. Department of Justice, 2006).

Once these programs were disclosed to the public, there was significant outcry over these warrantless wiretaps (Risen & Lichblau, 2005). Many argued these wiretaps were illegal and in violation of FISA or other federal law (Risen & Lichblau, 2005). One federal district court agreed, determining that the program violated the Constitution because it permitted searches without judicially authorized warrants (ACLU v. NSA, 2006). Instead of appealing the decision, the executive branch sought Congressional approval for the program. Congress eventually agreed to a modified version of the program and passed the FISA Amendment Act of 2008 (F.A.A.). But the legislative solution in response to the Terrorist Surveillance Program’s warrantless wiretaps had its own concerns, because it legislated an avenue for the government to obtain wiretaps without a judicially authorized search warrant (122 Stat. 2463, 2473).

Section 702 of the F.A.A. permits the executive branch to conduct warrantless wiretaps of foreign persons outside the United States to gather foreign intelligence (50 U.S.C. § 1881a(a) (2008)). While the FISC is involved, it does not approve individual surveillance, it merely approves the targeting and minimization procedures used generally by the intelligence community (50 U.S.C. § 1881a(a) (2008)). The FISC does not approve any individual interception, nor does it determine that there is probable cause that the interception will gather foreign intelligence information (50 U.S.C. § 1881a(a) (2008)).

Since the inception of Section 702 interceptions, there have been numerous mistakes, misuse and abuses of the program (Feinstein, 2012). 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 (Director of National Intelligence, 2013). There have also been systematic errors, where the collection system collects too much information because of technical errors that cannot be fixed (Director of National Intelligence, 2013). In short, the government has conceded that its collection process is flawed and a certain portion of its interceptions will be wholly domestic communications (50 U.S.C. § 1881a(a)). In other words, the program cannot be conducted without a small portion of its activity being outside of its permissible interception. So far, no court has ruled 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 instances of warrantless collection of information. The disclosure of classified surveillance programs by Edward Snowden created significant public outcry (Greenwald, 2013). 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 (Greenwald, 2013). 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 (50 U.S.C. § 1861).

The program leaked by Snowden was approved by the FISC but it nonetheless raised concerns similar to those found during the Church Committee 45 years earlier (Piette & Radack, 2006). The public concern was that current oversight of the government’s use of intelligence tools was insufficient to protect the liberties of everyday Americans (Greenwald, 2013). Public perception once again shifted to the belief that these intelligence tools were being misused to spy domestically on Americans with little connection to national security (Ball & Ackerman, 2013). The courts eventually weighed in, and the Second Circuit Court of Appeals has ruled that this bulk collection program is inconsistent with the statutory language of FISA, and thus, is unlawful (ACLU v. Clapper, 2015). Any information gathered from the bulk collection program is now likely inadmissible in a criminal prosecution as the fruit of an illegal search (50 U.S.C. 1806(e)).

Congress has responded to these concerns and eliminated the government’s bulk collection of limited information on Americans but has transferred this collection to private companies, who are required to retain information they collect and have it available for search (Kelly, 2015). 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.

VI. Planning for Change: What Intelligence Tools 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 tools will be lawful at the time of trial? This program was a statutory based (FISA Section 215) tool that had permission from multiple courts before it was ultimately ruled unlawful (In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted], 2015). 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 responding to current and future national security threats?

The answer involves risk analysis, something that is at the heart of intelligence analysis. But in today’s changing legal climate, national security professionals must conduct a risk analysis not only of the threats to the nation, but also analyze the risks that intelligence tools...
will become unavailable in the future. A careful review of the past and present controversies around intelligence collection demonstrate there are three factors that national security professionals can use to evaluate the risk of losing intelligence tools information gathered from them. These factors are: (1) whether knowledge of the tool is public or secret, (2) whether courts have issued approval of the use of the tool and (3) whether the intelligence tool resembles criminal tools that courts are comfortable with.

Classified sources and methods will eventually be made public—through leaks, declassification or other means (Kravets, 2013). National security professionals must accept this as fact. Each time one of the classified intelligence tools mentioned above was made public, there were negative consequences for the intelligence tool and the information gained from it (Donahue, 2013). The Terrorist Surveillance Program was leaked to the media and admitted to by the President (Risen & Lichblau, 2005). Subsequently, a district judge found the program to be unlawful (ACLU v. NSA, 2006). The Section 215 bulk data collection program was leaked by Edward Snowden—and a federal appellate court found it was unlawful (ACLU v. Clapper, 2015). The lesson from this is that programs that are entirely secret carry increased risk that upon disclosure they may be determined to be unlawful.

Many intelligence tools are well known, even though their use in a particular case is classified (50 U.S. C. §§ 1801-1805, 1861). Traditional FISA warrants are a perfect example (50 U.S. C. §§ 1801-1805). The program, the process to obtain them and their use are recognized and accepted by the Congress and the courts. These public intelligence tools carry less risk that they will be unavailable in the future.

Intelligence tools that require court approval carry less risk 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 (Executive Order 12,333). 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 to this point, but it actually proves the point (50 U.S.C. § 1861). The program was ruled to violate the statute, not comply with it (ACLU v. Clapper, 2015). The bulk collection program is an example of an intelligence tool that has risk of being lost because it was conducted in secret and without any corollary to a traditional criminal program (ACLU v. Clapper, 2015).

There is significantly less risk when using intelligence tools that have similarities to ordinary criminal investigative tools. When attempting to turn intelligence information into criminal evidence it helps to be working with an intelligence tool 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 (50 U.S. C. § 1805). 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 (Federal Rule of Criminal Procedure 41, 2015). 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. Courts are more likely to question the tool’s legality if it was not involved in the process to use the tool.

VII. Conclusion
Our nation has only begun to evaluate what changes to make to the intelligence tools available in our national security toolbox. 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 tools because the tools and their use will change. Some intelligence tools will be modified and restricted. Others will be removed by executive, legislative or judicial action.

Those charged with turning intelligence into evidence in criminal cases must be especially wary. The intelligence tools used today may be determined to be unlawful tomorrow. Any evidence gathered using those tools may not be admissible when the national security case comes to trial. But a cautious national security professional can carefully decide which of the currently available intelligence tools is likely to both meet the current collection requirement and also endure the current increased scrutiny so the information gathered is useful in the future. Doing so will ensure that tools being used to collect intelligence today will be able to be used to construct evidence for the criminal trial next year.
References

ACLU v. Clapper, 785 F.3d 787 (2nd Cir. 2015).
Executive Order 12,333.
In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [Redacted], No. BR 15–24 (Foreign Intel. Surv. Court, Feb. 26, 2015).
Major Patrick Walsh is an Associate Professor in the International and Operational Law Department of the U.S. Army Judge Advocate General’s Legal Center and School. Major Walsh is a military reservist currently serving on active duty. He deployed to Iraq in 2008 and served as a judge advocate advising commanders on international and operational law matters. As a civilian, Mr. Walsh is an Assistant U.S. Attorney in the District of Nevada, where he served as the lead national security and terrorism prosecutor for the district. He has also taught as an adjunct professor at the University of Nevada at Las Vegas, Boyd School of Law.

Major Walsh received his undergraduate degree from Loyola Marymount University, his law degree from the University of California at Berkeley, Boalt Hall School of Law and his L.L.M. in Military Law with an emphasis in International and Operation Law from the U.S. Army’s Judge Advocate General’s Legal Center and School. He teaches courses on Terrorism and the Law, National Security Law, the Domestic Operations of the Military and Reserve Component Affairs.