



PROGRAM MATERIALS

Program #2946

March 28, 2019

FISA: More of Everything You Didn't Know

**Copyright ©2019 by George Croner, Esq., Foreign Policy
Research Institute (FPRI). All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969



FISA: MORE OF EVERYTHING YOU DIDN'T KNOW, YOU DIDN'T KNOW

George W. Croner | Senior Fellow | FPRI.org

SOME TERMINOLOGY

- “FISA” is the Foreign Intelligence Surveillance Act
- Signals intelligence OR “SIGINT” is the monitoring, interception, and interpretation of radio transmissions, radar signals, or telemetry.
- Two subsets of SIGINT: Communications Intelligence (COMINT) focuses on extracting intelligence from communications between people while Electronic Intelligence (ELINT) focuses on extracting intelligence from electronic signals not directly used in communication
- Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. “Cryptology” is the study of cryptography.

SOME HISTORY

- The use of electronic communications by governments for military and diplomatic purposes led to cryptographic efforts by users to secure their communications and corresponding efforts by adversaries to break those encryptions and exploit the communications.
- World War I and the “Zimmerman Telegram” - a British cryptographic success that may have changed the course of the war

SOME HISTORY, CONT'D

Between the World Wars

- The Cipher Bureau a/k/a the “Black Chamber” - Herbert Yardley, America’s first great cryptologist
- Cryptanalytic efforts by the Black Chamber contributed greatly to U.S. knowledge of Japanese intentions during the 1921 Washington Naval Conference but Henry Stimson, Secretary of State, in 1929 ends funding for the Black Chamber asserting that “Gentlemen do not read each other’s mail.”

SOME HISTORY, CONT'D

World War II

World War II successes in communications intelligence (e.g., Bletchley Park/ENIGMA and cryptologic successes against Japanese communications (MAGIC)) demonstrated the importance of signals collection and cryptographic efforts.

SOME HISTORY, CONT'D

The Cold War

Asymmetric struggles of the Cold War and potential for nuclear confrontation increased the importance of signals intelligence efforts.

[\[click here to view the Venona Decrypts\]](#)

PRESIDENTIAL AUTHORITY

- Presidents from Franklin Roosevelt to Richard Nixon authorized the use of electronic surveillance, both domestically and abroad, to acquire foreign intelligence and protect national security.
- Surveillance was conducted without specific legislative authority and authorization was premised on the President's constitutional authority as both commander-in-chief and as the government's principal authority in the conduct of foreign affairs.
- In 1952, by secret directive, President Truman created the National Security Agency and all U.S. signals intelligence and cryptologic efforts were consolidated under the aegis of NSA. NSA was, and is, the principal U.S. agency authorized to conduct signals intelligence activities.
- For the first 25 years of its existence, the U.S. government did not officially acknowledge the existence of NSA and, while Congress exempted NSA's activities from virtually any reporting or disclosure obligation, it enacted no laws regulating what NSA actually did.

[\[Click here to view the National Security Agency Act of 1959\]](#)

KEITH AND POST-WATERGATE DEVELOPMENTS

Congress and the Courts Get Involved: Title III and U.S. v. U.S. District Court (the Keith case)

- Berger v. NY and Katz v. U.S. (both decided in 1967) bring electronic surveillance squarely within the coverage of the Fourth Amendment and create the concept of a “reasonable expectation of privacy”
- Congressional response is Title III of the 1968 Omnibus Crime Control and Safe Streets Act creating a warrant requirement based on Fourth Amendment standards for all non-consensual law enforcement electronic surveillance
- Title III is specifically neutral on the division of authority or requirements for electronic surveillance conducted for foreign intelligence or national security purposes
- After congressional passage of Title III, Keith (decided in 1972) represents the Supreme Court’s first statement addressing presidential authority to direct warrantless surveillance for national security purposes. Court rules that a warrant is required for any domestic surveillance even if undertaken for “national security” purposes.

[\[Click here to view the court documents from the Keith case\]](#)



THE CHURCH AND PIKE COMMITTEE INVESTIGATIONS (1975)

- Congress investigates U.S. intelligence activities - it isn't pretty
- NSA's existence is publicly confirmed for the first time - Shamrock and Minaret collection programs are publicly revealed
- Congress passes the Foreign Intelligence Surveillance Act of 1978

THE BASIC CONSTRUCT OF “TRADITIONAL” FISA

When Does FISA Apply and What Showing is Required for a FISA Order?

- “Traditional” FISA refers to Title I which covers what most people would generally envision as foreign intelligence electronic surveillance
- Traditional FISA surveillance frequently turns on definitional interpretations since the basic construct of FISA is that electronic surveillance may not target a U.S. person or be conducted against anyone in the United States without an order from the Foreign Intelligence Surveillance Court (“FISC”) issued upon a finding of probable cause that the surveillance is undertaken to acquire foreign intelligence and that the target of the surveillance is a foreign power or an agent of a foreign power
- Under FISA, the only time electronic surveillance can be conducted in the United States without a warrant is where the Attorney General certifies in writing that (1) the surveillance is directed only against communications facilities used solely between or among foreign power(s), and (2) there is no substantial likelihood that the surveillance will acquire the communications of U.S. persons
- FISA defines “electronic surveillance” in four ways and each definition turns upon an effort to acquire the “contents” of a communication. (50 U.S.C. § 1801(f) - [\[Click here to view A copy of FISA in it's current form\]](#)

THE BASIC CONSTRUCT OF “TRADITIONAL” FISA

The Foreign Intelligence Surveillance Court

- The Foreign Intelligence Surveillance Court (“FISC”) was established by FISA. Today, it consists of 11 judges drawn from the U.S. district courts and appointed by the Chief Justice. The court must be comprised of judges drawn from at least 7 different judicial districts and 3 of the judges selected must reside within 20 miles of the District of Columbia. FISC operates out of a secure facility in the U.S. Courthouse in Washington, D.C.
- FISA also created a Foreign Intelligence Surveillance Court of Review (FISCR) consisting of three judges appointed by the Chief Justice and drawn from the U.S. district courts or courts of appeal. The FISA court of review convened for the first time in 2002 to hear an appeal by the government from a denial of a surveillance application by the FISC.
- The FISC was created by Congress to restore a measure of checks and balances to the area of electronic surveillance conducted for foreign intelligence purposes. Conceptually, the FISC is intended to serve the “neutral and detached magistrate” role that judicial officers play under Title III in connection with electronic surveillances for law enforcement purposes.
- The workload of the FISC has increased dramatically over the years. In 1980, its first full year of operation, the FISC received 322 applications for electronic surveillance and approved each one. By 2018, the Administrative Office of U.S. Courts (AOUSC) reported that the FISC had received 1,339 applications for authority to conduct “traditional” FISA surveillance in 2017

[\[Click here to view a copy of my article “THE 2017 FISA REPORTING SEASON HAS ENDED: WHAT DO THE NUMBERS MEAN?”\]](#)

THE EXPANSION OF FISA THROUGH THE 1980'S

Physical Searches and Pen Register/Trap and Trace Devices

- In 1995, FISA was amended to include physical searches undertaken for foreign intelligence purposes. This authority permitted the physical search of premises by order of the FISC upon a showing of probable cause showing that: (a) the target of the search is a foreign power or an agent of a foreign power; (b) the premises searched contain foreign intelligence information; and (c) the premises to be searched is owned, used, or possessed by a foreign power or agent of a foreign power.
- In 1998, FISA was further amended to permit, upon approval by the FISC, the installation and use of pen register (recording outgoing call information) and/or trap and trace (recording incoming call information) devices for foreign intelligence purposes.
- In the case of these devices, the Attorney General (or appropriate designee) must certify that the information sought is in connection with investigation of “foreign intelligence information not concerning a U.S. person,” or “to protect against international terrorism or clandestine intelligence activities.”

POST-9/11 CHANGES AND AMENDMENTS TO FISA

“Stellar Wind” and The USA PATRIOT Act Ultimately Lead to FISA Section 702

- After 9/11, it became clear that, while FISA had remained substantively static nearly three decades, world events and evolving telecommunications had not
- Telecommunications technology and accompanying changes in infrastructure altered the communications environment in ways unanticipated when FISA was enacted in 1978. For example, FISA contemplated an environment in which most local (i.e., domestic) communications would be carried by wire while the majority of international communications would be transmitted via radio. By the early 2000s, however, the shift to undersea cables (generally fiber optic) for international communications and the vastly expanded domestic cellular network had essentially reversed FISA's technological assumptions - this change adversely impacted NSA's conduct of its signals intelligence mission after 9/11
- To address the intelligence needs directed towards the terrorist threat environment following 9/11, President George W. Bush secretly implemented the highly classified “Terrorist Surveillance Program” (TSP), codenamed ‘Stellar Wind’ in which NSA conducted the warrantless collection of both the contents of certain international communications and, in bulk, non-content (i.e., “metadata”) about telephone and internet communications

POST-9/11 CHANGES AND AMENDMENTS TO FISA

“Stellar Wind” and The USA PATRIOT Act Ultimately Lead to FISA Section 702

- Following the 9/11 attacks, Congress passed the Patriot Act and articulated its desire to enhance the sharing of intelligence among federal agencies, strengthen the criminal laws against terrorism, remove obstacles to investigating terrorism, and update the law to accommodate new technology
- In pursuit of those objectives, FISA was amended to remove the requirement that the collection of foreign intelligence be the purpose of a surveillance to requiring that the applicant for a FISA order certify that the acquisition of foreign intelligence was a significant purpose of the surveillance
- In 2002, the “wall” that had long separated foreign intelligence surveillance information from law enforcement use was removed. Citing Congress’s desire for greater integration of intelligence and law enforcement efforts post-9/11, the DoJ sought to eliminate, with respect to international terrorism cases, the existing minimization procedures forbidding the sharing of foreign intelligence information with law enforcement components. The FISC initially demurred precipitating the first-ever appeal to the Foreign Intelligence Surveillance Court of Review. That court reversed the FISC and, as one commentator observed, “the ‘Wall’ tumbled into a grave well dug for it by the Court of Review.’”

POST-9/11 CHANGES AND AMENDMENTS TO FISA

“Stellar Wind” and The USA PATRIOT Act Ultimately Lead to FISA Section 702

- In 2005, after public disclosures of the existence of the TSP, the government pursued authorization for the same collection from the FISC but the fluidity of suspected terrorists' movements and the rapidity with which they changed communications facilities created surveillance challenges under the existing FISA structure
- In 2008, after receiving information that current authorities (e.g., the Patriot Act and the Protect America Act) as interpreted and applied by the FISC had left an “intelligence gap” in the nation's foreign intelligence collection, Congress further amended FISA to authorize additional procedures for the targeting of persons outside the United States. This is the authority that is now known as “Section 702 collection” (50 U.S.C. § 1881a).

FISA SECTION 702 - TARGETING PERSONS ABROAD WITHOUT A WARRANT

The Basic Construct of Section 702

- First enacted as part of a major series of amendments to FISA in 2008, Section 702 was renewed in 2012 and, after extended debate, was renewed again in January 2018. Current authority expires December 31, 2023.
- Under Section 702, the Attorney General and the DNI may jointly authorize the targeting of persons reasonably believed to be located outside the U.S. to acquire foreign intelligence information
[**\[Click here to view a copy of my article “THE CLOCK IS TICKING: WHY CONGRESS NEEDS TO RENEW AMERICA’S MOST IMPORTANT INTELLIGENCE COLLECTION PROGRAM”\]**](#)
- Approval for such targeting is acquired by means of a Certification submitted to the FISC that attests that any acquisition of communications will be made in accordance with “targeting” procedures, minimization procedures, and guidelines established by the Attorney General. The targeting and minimization procedures are submitted to the FISC for review to insure they conform with the requirements of FISA and with the Fourth Amendment.

FISA SECTION 702 - TARGETING PERSONS ABROAD WITHOUT A WARRANT

The Basic Construct of Section 702

- Unlike a “traditional” FISA surveillance, however, there is no individualized targeting determination submitted for approval by the FISC nor is any probable cause determination made by the FISC.
- Absence of an individualized P/C determination means the government uses a single certification to authorize acquisitions related to multiple types of foreign intelligence information. For example, in 2017, the government used a single certification approved by the FISC as support for acquisitions targeting 129,080 foreign targets.

702 STATISTICS

“Traditional FISA and Sections 703 and 704”	CY 2013	CY 2014	CY 2015	CY 2016	CY 2017
Total FISA Orders	1,767	1,519	1,585	1,559	1,437
Est. # of targets	1,144	1,562	1,695	1,687	1,337
Est # of U.S. Person targets	N/A	N/A	N/A	336	299

FISA Section 702	CY 2013	CY 2014	CY 2015	CY 2016	CY 2017
Total # FISC Orders	1	1	1	0	1
Estimated Total # of Targets	89,138	92,707	94,368	106,469	129,080

Sources: (1) Director of National intelligence *Statistical Transparency Report* (2018)
(2) Reporting of the Administrative Office of U.S. Courts (2018)

FISA SECTION 702 - TARGETING PERSONS ABROAD WITHOUT A WARRANT

The Basic Construct of Section 702

- Once the FISC has entered an order approving the Certification, the government conducts the acquisition by directing the assistance of an “electronic communication service provider” which is immediately required to provide the government with all assistance necessary to accomplish the acquisition in a manner that will protect its secrecy while producing minimum interference with the provider’s service to the target.
- Notwithstanding the foreign focus of the targets of Section 702 surveillance, the acquisition of communications under Section 702 occurs in the United States, and the statute specifically provides that the Attorney General and the DNI may direct an electronic communication service provider to provide the assistance needed to effectuate the surveillance.
- **SECTION 702 AUTHORITY CAN NEVER BE USED TO TARGET THE COMMUNICATIONS OF, OR DIRECT COLLECTION AGAINST, A U.S. PERSON**

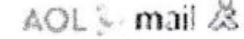
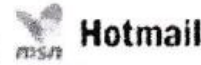
FISA SECTION 702 - TARGETING PERSONS ABROAD WITHOUT A WARRANT

Foreign Focus - U.S. Impact

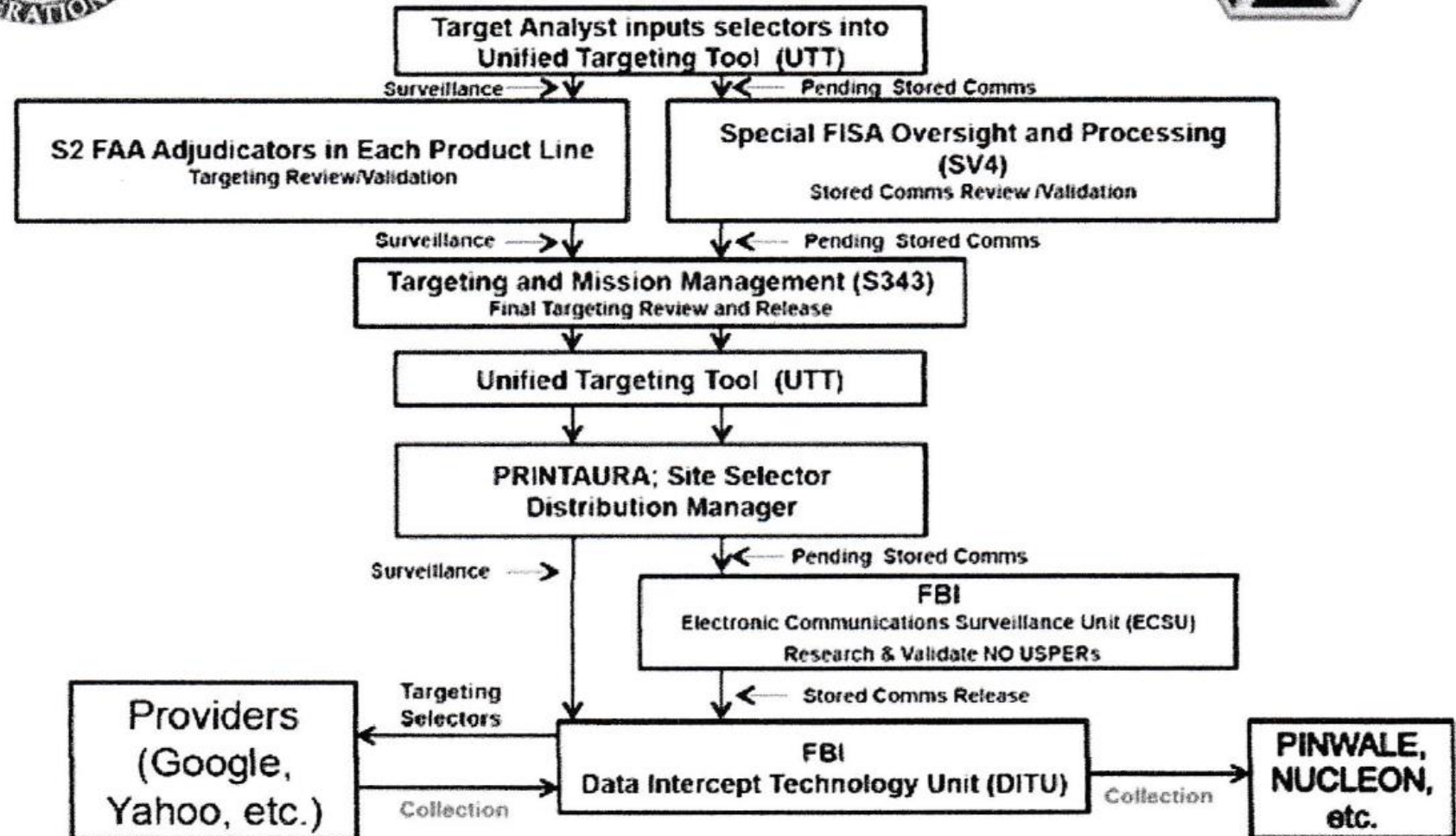
- Section 702 collection could not be conducted without a warrant under Title I of FISA but is specifically excepted from Title I requirements (50 U.S.C. § 1881a(c)(4))
- Communications are obtained with cooperation of U.S. Internet Service Providers (Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, and Apple) or “backbone” communications companies (e.g., AT&T and Verizon)
- Two forms of 702 collection (PRISM (i.e., “Downstream”) and Upstream

PRISM TASKING

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) PRISM Tasking Process



TOP SECRET//SI//ORCON//NOFORN

FISA SECTION 702 - TARGETING PERSONS ABROAD WITHOUT A WARRANT

Foreign Focus - U.S. Impact

- Principal focus of 702 opponents: although only foreign “persons” are targets, collection obtains communications of any U.S. person communicating with a foreign target
 - such collection is considered “incidental” and does not required a separate warrant
- U.S. person communications can be queried as part of intelligence production from 702 collection
 - multiple statutory and regulatory restrictions governing queries that produce U.S. person communications and use of such information

[\[Click here to view a copy of the THE 2016 NSA SECTION 702 MINIMIZATION PROCEDURES\]](#)

- Importance of Section 702 collection
 - scope of this collection (hundreds of millions of internet communications are collected annually) activity means that nearly 25% of all NSA’s counterterrorism reporting is derived from Section 702 collection
 - another measure showed that an average of 4 items per day derived from Section 702 collection appeared in the President’s daily intelligence brief
 - more recently, NSA’s Director informed Congress that “much — not all, much of what was in the intelligence community’s assessment, for example, on the Russian efforts against the U.S. election process in 2016 was informed by knowledge we gained through 702 authority”

FISA IN THE NEWS

The HPSCI “Investigation” and the Carter Page FISA Controversy

- For nearly a year, the Republican majority on the House Permanent Select Committee for Intelligence has been pursuing allegations that the FBI and the Justice Department manipulated and deceived the FISC to obtain authority to surveil former Trump foreign policy advisor Carter Page using the “Steele Dossier” [\[Click here to view a copy of the “Steele Dossier”\]](#)
- Controversy stems from 4 applications granting FISA authority to surveil Page and has pushed FISA and the FISA process into the news
- One result was the first public release ever of FISA applications (albeit heavily redacted) [\[Click here to view a copy of the Carter Page FISA Application\]](#)
- Serious people have pointed to the Page application scenario and called for the abolition of the Foreign Intelligence Surveillance Court [\[Click here to see a copy of the Wall Street Journal Op/Ed expressing this opinion – and my response “The FISA Court’s Essential Purpose”\]](#)
- The debate also has included less serious hyperbole about the Carter Page FISA controversy which is the subject of my article “OutFoxed - The Vulpine Network Keeps Swinging and Missing at the Carter Page FISA Applications” [\[click here to view the article\]](#)

LINKS TO REFERENCED DOCUMENTS

- [Verona Decrypts](#)
- [National Security Agency Act of 1959](#)
- [The Keith Decision](#)
- [FISA in its Current Form](#)
- [The 2017 FISA Reporting Season Has Ended: What do the Numbers Mean?](#)
- [The Clock is Ticking: Why Congress Needs to Renew America's Most Important Intelligence Collection Program](#)
- [2016 NSA Section 702 Minimization Procedures](#)
- [Steele Dossier](#)
- [Carter Page FISA Applications](#)
- [Wall Street Journal Op/Ed](#)
- [The FISA Court's Essential Purpose](#)
- [OutFoxed – The Vulpine Network Keeps Swinging and Missing at Carter Page FISA Applications](#)