PROGRAM MATERIALS
Program #32267
November 30, 2022

# Electronic Surveillance in the U.S. for National Security Purposes – The History, Purpose and Future of the Foreign Intelligence Surveillance Act



Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

*"Electronic Surveillance in the U.S. for National Security Purposes – The History, Purpose and Future of the Foreign Intelligence Surveillance Act"*

## I. Electronic Surveillance for Foreign Intelligence Prior to FISA [20 minutes]

A. Some Basic 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.
- Three subsets of SIGINT: Communications Intelligence (COMINT) focuses on extracting intelligence from communications between people; Electronic Intelligence (ELINT) focuses on extracting intelligence from electronic signals not directly used in communication; and FISINT (foreign instrumentation signals intelligence) extracts electronic intelligence from foreign weapon systems.
- Cryptography is the practice and study of techniques for secure communication in the presence of adversaries. "Cryptology" is the study of cryptography.

B. Pre-FISA History of Electronic Surveillance for Foreign Intelligence

- 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 (opportunity created by severing all international cables connecting Germany to U.S. hours after the outbreak of WWI)

- Between the World Wars

    i. the Cipher Bureau a/k/a the "Black Chamber" - Herbert Yardley, America's first great cryptologist

    ii. 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."

    iii. Elizabeth and William Friedman – married in 1917 and worked both together and separately as the greatest "cryptanalytic couple" in history. William was instrumental in the breaking of the Japanese "Purple" code and was one of the founding fathers of the National Security Agency. Elizabeth worked for a variety of government agencies and was instrumental in breaking the codes used by international crime groups to smuggle alcoholic beverages into the U.S. during Prohibition

- World War II

    i. World War II successes in communications intelligence (e.g., Bletchley Park/ENIGMA (ULTRA) and cryptologic successes against Japanese communications (MAGIC)) demonstrated the importance of signals collection and cryptographic efforts [The film "The Imitation Game" chronicles the British effort to break the German Enigma system during WWII.]

- The Cold War

    i. asymmetric struggles of the Cold War and the potential for nuclear confrontation increased the importance of signals intelligence efforts to better understand and anticipate the motives and actions of U.S. adversaries (particularly the Soviet Union)

    ii. VENONA [**VENONA DECRYPTS ARE IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION**]

        1. Initial Venona success contributed to U.S. handling of the Berlin crisis and Berlin airlift of 1948-49
        2. But success was short-lived when William Weisband, a mid-mid-level linguist at the predecessor of NSA betrayed Venona's success to the Soviets. On ***Black Friday*** **(October 29, 1948),** based on Weisband's information, the Soviets instituted massive changes in their cipher systems, radio networks, operating frequencies, communications security disciplines, and radio calls signs. These changes served

to frustrate American cryptanalysts for the better part of the next 3 decades (until the 1970s) demonstrating the fragility of COMINT and its sources and methods. ANOTHER EXAMPLE OF THAT FRAGILITY, WEISBAND WAS NEVER TRIED BECAUSE THE DISCLOSURES NECESSARY TO CONDUCT SUCH A TRIAL WOULD HAVE POSED TOO GREAT A RISK TO COMINT SOURCES AND METHODS. INSTEAD, HE DIED OF A HEART ATTACK WHILE ON THE WAY TO THE SMITHSONIAN INSTITUTE WITH HIS CHILDREN IN 1967 - NEARLY 20 YEARS AFTER HIS BETRAYAL.

## II. The History of Presidential Authority [10 minutes]

A. Presidents from Franklin Roosevelt to Richard Nixon unilaterally authorized the use of electronic surveillance, both domestically and abroad, to acquire foreign intelligence and protect national security.

- FDR authorized electronic surveillance for national security purposes even when the Supreme Court had explicitly declared electronic surveillance illegal under the Communications Act of 1934 (**U.S. v. Nardone**) [**FDR MEMO RE ELECTRONIC SURVEILLANCE FOR NATIONAL SECURITY PURPOSES IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION**]

B. 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.

C. 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. (Contrast to the CIA which was formed by legislative enactment (the National Security Act of 1947)).

- 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. [THE MATERIALS LISTED AT THE END OF THE PRESENTATION INCLUDE A LINK TO THE NATIONAL SECURITY AGENCY ACT OF 1959]

## III. *Keith* and Post-Watergate Developments [15 minutes]

A. 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. [A COPY OF THE *KEITH* DECISION IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION]

    i. In the midst of calls for abolishing the FISC, does *Keith* require that a comparable alternative replace the FISC?/Could Congress, if it was so inclined, return authority for foreign intelligence surveillance conducted in the U.S. solely to the discretion of the president?

B. 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 [A LINK TO THE FISA STATUTE IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION]

## IV. The Basic Construct of "Traditional" FISA [25 minutes]

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

- "Traditional" FISA refers to Title I of FISA which covers what most people would generally envision as electronic surveillance conducted *in the United States* for foreign intelligence purposes – Emphasis is on ***in the United States*** – electronic surveillance conducted outside the United States, other than when specifically targeting U.S. Persons, is governed by Executive Order 12333.

- 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 when the Attorney General, acting on behalf of the president, 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.

B. 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 (a "SCIF") 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 FISCR convened for the first time in 2002 to hear an appeal by the government from a denial of a surveillance application by the FISC.

    i. The appeal was In re Sealed Case, 310 F.3d 717 (FISCR 2002) which, relevant to more recent events occurring in connection with the Carter Page FISA applications, essentially involved the FISC seeking to impose its own set of "additional" minimization requirements to maintain the "Wall" that existed at the time between law enforcement and foreign intelligence/counterintelligence surveillance. At the time, the FISC had lost all confidence in the credibility of the FBI's FISA applications (sound familiar?) and insisted upon imposing its own set of additional restrictions on FBI surveillance applications in the form of supplemental minimization requirements. The FISCR

concluded that the FISC had no authority to impose such additional requirements and that, in fact, there was no requirement in FISA for "the Wall" that the Justice Department had created to separate law enforcement activities from counterintelligence functions.

- 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 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 2020 (CY2019), DNI's Annual Statistical Transparency Report shows the FISC issuing 907 "probable cause" orders (for "traditional" Title I FISA surveillance or physical searches) (which actually represented a decrease from the 1,184 "probable cause" orders reported by the DNI in CY 2018.)

- For reasons that are not entirely clear, the numbers continued to drop in CY2020 and in CY2021 when only 524 "probable cause" orders were issued. Whether this is a reflection of more scrupulous vetting by the Executive Branch (after the DoJ IG Report on abuses (the "Horowitz Report") following the controversy over the Carter Page FISA applications or operational reasons, there has been a material decline in the number of FISA orders issued in recent years. [A LINK TO THE LAWFARE ARTICLE ON THE DECLINE IN THE USE OF NATIONAL SURVEILLANCE AUTHORITIES IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION]

## V. The Expansion of FISA through the 1990s [5 minutes]

A. 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."

## VI. Post-9/11 Changes and Amendments to FISA [20 minutes]

A. 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 ( AUTHORIZING THE COLLECTION OF PHONE AND INTERNET COMMUNICATIONS WITH ONE TERMINUS IN THE U.S. WITHOUT A COURT ORDER VIOLATED FISA}

- 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).

## VII. FISA Section 702 - Targeting Persons Abroad [25 minutes]

### A. 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 [A LINK TO THE ARTICLE "THE CLOCK IS TICKING: WHY CONGRESS NEEDS TO RENEW AMERICA'S MOST IMPORTANT INTELLIGENCE COLLECTION PROGRAM" IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION]

- 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 (1) "Targeting" Procedures, (2) Minimization Procedures, (3) Querying Procedures, and (4) "Guidelines" established by the Attorney General. The Targeting, Minimization, and Querying Procedures

are submitted to the FISC for review to insure they conform with the requirements of FISA and with the Fourth Amendment.

- Targeting Procedures – designed to (1) ensure targeting is limited to non-U.S. persons reasonably believed to be located outside the U.S.; (2) prevent the intentional acquisition of communications where sender and all recipients are in U.S, at time of acquisition.

- Minimization Procedures – designed to limit the public dissemination of nonpublic information concerning nonconsenting U.S. persons (Use of "Masking "to protect U.S. Person Identities)

- Querying Procedures – scope of Querying of unminimized data using U.S Person identifiers – FBI ran approx. 3.1 million queries against unminimized FISA data in CY 2017 (as compared to roughly 7500 combined run by NSA and CIA)

- 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. [**LINK TO Section 702 Materials LISTED AT THE END OF THE PRESENTATION**]

- The key differences between "traditional" Title I FISA surveillance and Section 702 (§ 1881a) are essentially found in 2 provisions of Section 702:

    - Section 702(c)(4) "Nothing in title I shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this

section at a person reasonably believed to be located outside the United States." — **NO INDIVIDUALIZED PROBABLE CAUSE ORDER IS REQUIRED IF AN ACQUISITION IS PROPERLY TARGETED UNDER SECTION 702**

- Section 702(h)(4) "A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted." —**NO PARTICULARIZED IDENTIFICATION OF THE FACILITIES, PLACES, PREMISES OR PROPERTY TARGETED IS REQUIRED**

- 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 CY2021, the government used a single certification approved by the FISC as support for acquisitions targeting ***232,432*** foreign targets. [**LINK TO THE DNI STATISTICAL TRANSPARENCY REPORT FOR CY 2022 IS IN THE MATERIALS LISTED AT THE END OF THE PRESENTATION**]. **In CY 2013, the first year the DNI was required to publicly disclose this statistical information, the number of targets was 89,138.**

- 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

B. Incidental Collection and Querying the Section 702 Database

- 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

- Principal focus of 702 opponents: although only foreign "persons" are targets, collection obtains communications of any U.S. person communicating with a foreign target

    1. such collection is considered "incidental" and does not require a separate warrant

    2. U.S. person communications can be queried as part of intelligence production from 702 collection/use of U.S. person query terms against unminimized Section 702 data is highly regulated and each term used is specifically recorded by technical means

3. multiple statutory and regulatory restrictions govern queries that produce U.S. person communications and use of such information

C. Legal Challenges to Section 702

- *Clapper v. Amnesty International*
- *Wikimedia v. National Security Agency*
- *U.S. v. Muhtorov*
- *U.S. v. Mohamud*
- *U.S. v. Hasbajrami*

## QUESTIONS AND WRAP UP

# LIST OF MATERIALS FOR FISA COURSE (NOVEMBER 2022)

**Venona Exhibits -**
**https://drive.google.com/open?id=19x5GPte0FoaSzL5D41a9tVznL6nC6UcM&authuser=dede%40dsavirtualworld.com&usp=drive_fs**

**FDR Memo Re: Electronic Surveillance for National Security Purposes -**
**https://drive.google.com/open?id=18XGmqVGJw52oUvOnTXSauT8Us-u0ks-s&authuser=dede%40dsavirtualworld.com&usp=drive_fs**

**National Security Agency Act of 1959 –**
**https://drive.google.com/open?id=1FwHSaTBiBGmJlLwi6ZdxSD-QrBaC1G_O&authuser=dede%40dsavirtualworld.com&usp=drive_fs**

**The *Keith* Decision – https://drive.google.com/open?id=1A2ZzbNYTX77AnuX-tMeSYKIH9tBsxsPA&authuser=dede%40dsavirtualworld.com&usp=drive_fs**

**The FISA Statute –**
**https://drive.google.com/open?id=1A9zJtqKcRaRSQNPLc6ysw_qLlSci_vku&authuser=dede%40dsavirtualworld.com&usp=drive_fs**

**Lawfare Article Addressing Recent Decline in Use of National Surveillance Authorities: New Statistics Confirm the Continuing Decline in the Use of National Surveillance Authorities**

**Article: "The Clock is Ticking: Why Congress Needs to Renew America's Most Important Intelligence Collection Program" –**
**https://www.fpri.org/article/2017/09/clock-ticking-congress-needs-renew-americas-important-intelligence-collection-program-parts-i-iv/**

**Director of National Intelligence Annual Statistical Transparency Report:**
**https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf**

**FISC OPINION APPROVING SECTION 702 PROCEDURES (November 18, 2020):**
**https://www.washingtonpost.com/context/ruling-on-fbi-s-warrantless-surveillance-powers/0c460a9e-8571-4626-b5ce-f4e9d311c8d4/?itid=lk_interstitial_manual_20**

**SECTION 702 DETAILS –**
**https://drive.google.com/open?id=18uKrywttv_5g9zvXYo6-4H-ZzKpIz7Do&authuser=dede%40dsavirtualworld.com&usp=drive_fs**