The FISA Amendments Act: Q&A

The Intelligence Community's top legislative priority for 2017 is reauthorization of the FISA Amendments Act.

The FISA Amendments Act (FAA), codified as Title VII of the Foreign Intelligence Surveillance Act (FISA) authorizes foreign intelligence surveillance activities that have been vital to keeping the nation safe. It will sunset on December 31, 2017 unless Congress passes legislation to remove or extend the sunset provision. Title VII includes not only Section 702, which concerns targeting non-United States (U.S.) persons[1] abroad for surveillance, but also Sections 703, 704 and 705, which concern and provide statutory procedures and protections for surveillance of U.S. persons abroad. Section 702 has been the subject of significant discussion over the last several years and is the focus of this paper.

Title VII of FISA permits the government to acquire foreign intelligence information about the plans and identities of terrorists and terrorist organizations, including how they function and receive support. It enables collection of foreign intelligence information about the intentions and capabilities of spies, weapons proliferators and other foreign adversaries who threaten the United States, and it informs U.S. Intelligence Community (IC) cybersecurity efforts. Allowing the FAA to sunset would greatly impair the ability of the United States to respond to national security threats and to respond to foreign intelligence collection opportunities. Further, the additional protections established by Title VII for U.S. persons located abroad would expire with the FAA sunset.

What is the Foreign Intelligence Surveillance Act?

FISA was originally enacted in 1978 to provide the Executive Branch with a court-authorized process for conducting four specific types of electronic surveillance against foreign powers or their agents operating inside the United States. The statute is still used for that original purpose, but has been amended a number of times to provide a comprehensive statutory vehicle for certain additional types of court-authorized foreign intelligence collection. Congress added Title VII of FISA in 2008 to permit additional procedures for targeting certain persons located outside the United States with surveillance. Congress reauthorized the FAA in 2012.

What is Traditional FISA?

Titles I and III of FISA are often called "Traditional FISA." These provisions apply, respectively, to the conduct of electronic surveillance and physical searches for foreign intelligence purposes of persons, facilities, or property inside the United States. Under Title I, the government files a detailed application asking the Foreign Intelligence Surveillance Court (FISC) to authorize the electronic surveillance of a facility (*e.g.*, a telephone number or email account) or place. For this request to be granted, the government must show **probable cause** to believe both that the proposed target is a foreign power or an agent of a foreign power and that the facility or place is or is about to be used by that target. Under Title III, the government files a

[1] U.S. persons are U.S. citizens or lawful permanent residents of the United States, as well as U.S. corporations and unincorporated associations where a substantial number of members are U.S. persons (unless the corporation or association is a foreign power). For purposes of this paper, "foreign target" or "foreign person" includes any entity that does not meet this U.S. person definition.

similar application seeking authority to search premises or property that is or is about to be owned, used, possessed by, or in transit to or from a foreign power or an agent of a foreign power. If the FISC agrees that there is probable cause and that the government's proposed collection techniques and minimization procedures adequately protect U.S. person information acquired in the course of the collection activity, then the FISC grants the government authority to conduct the electronic surveillance or physical search.

Of note, this requirement for a judicial order based on probable cause is intended to protect the constitutional rights of U.S. persons and persons inside the United States against unreasonable searches and seizures. The Constitution does not require this practice for foreign persons located abroad.

Why was FISA amended in 2008 through enactment of the FAA?

When Congress enacted FISA in 1978, it drafted the law so that foreign persons located outside the U.S. would be outside of FISA's ambit. This was accomplished in large part by defining electronic surveillance based on the technology of 1978. However, by 2008, technology had changed considerably and many terrorists and other foreign intelligence targets abroad were using communications services based in this country, especially those provided by U.S.-based Internet service providers (ISPs).

This change in technology and methods of communication meant that under FISA, as it was constructed before the FISA Amendments Act (FAA), the government often had to obtain a Traditional FISA order to compel U.S.-based ISPs to provide to the government communications of foreign persons located abroad, such as communications of a foreign terrorist using a U.S.-based ISP. As a result, in many instances, the same processes were used to conduct surveillance on foreign persons located abroad – including demonstration of probable cause – as were required to conduct surveillance on U.S. persons and persons inside the U.S. This result proved very costly. First, the significant resource demands of obtaining judicial approval for FISA surveillance meant that the government was unable to process Traditional FISA orders for numerous foreign intelligence targets outside the United States. Instead, the government prepared Traditional FISA applications for a relatively small subset of the highest-priority targets, leaving many valid foreign intelligence targets, including terrorists, outside the reach of surveillance. Second, in some instances—including high-priority cases—the government could not establish that the foreign targets met the statutory requirements intended to protect U.S. persons and persons inside the United States, including the probable cause requirements.

To address these unanticipated effects of changing technologies, and after many months of effort and public debate, Congress enacted Section 702 of FISA as part of the 2008 FAA with significant bipartisan support. It was reauthorized in 2012, again with significant bipartisan support.

What does FISA Section 702 permit the U.S. Government to do?

SUMMARY

As described in more detail below, Section 702 permits the government to target for surveillance foreign persons located outside the United States for the purpose of acquiring foreign intelligence information (with the compelled assistance of electronic communication service providers) while also providing a comprehensive oversight regime by all three branches of government to protect the constitutional and privacy interests of any U.S. person whose information may be incidentally acquired during the collection activity.

Generally, Section 702 permits the Attorney General (AG) and the Director of National Intelligence (DNI) to authorize the IC to target foreign persons reasonably believed to be located outside the U.S. for the purpose of acquiring foreign intelligence information. This acquisition is conducted pursuant to a FISC order approving a certification and accompanying targeting and minimization procedures. As described in further detail below, these documents regulate the government's use of Section 702 and provide protections for U.S. persons. The IC acquires this foreign intelligence information with the compelled assistance of electronic communication service providers, as directed by the AG and the DNI.

Instead of issuing individual court orders, the FISC approves annual **certifications** submitted by the AG and the DNI that specify categories of foreign intelligence information, as defined by FISA, that the government is authorized to acquire pursuant to Section 702. The Office of the DNI (ODNI) has publicly released a sample of a certification, with required supporting documents, on its website *IC on the Record*.[2]

The AG and the DNI must also certify that IC elements will follow **targeting procedures** and **minimization procedures** that are approved by the FISC as part of the annual package.

- The **targeting procedures** are designed to ensure that only foreign persons located outside the U.S. are targeted for foreign intelligence collection purposes.
- The **minimization procedures** are intended to protect any U.S. person information that is incidentally acquired in the course of Section 702 collection. Like all other forms of legal authority that permit the government to target someone for foreign intelligence collection, Section 702 authorizes collection of communications sent or received by the target—in other words, the collection will generally include information sent to the target from other communicants and vice versa. As Congress understood when it passed the FAA, and as is true with any form of surveillance, a foreign person who has been targeted for collection under FISA Section 702 may communicate with, or discuss information concerning, a U.S. person. This is considered "incidental" acquisition of the information concerning the U.S. person, as the U.S. person was not the target of collection. Protection of this incidentally acquired U.S. person information is the reason why Congress requires minimization procedures for Section 702 collection. FISC approved minimization procedures regulate the retention and dissemination of information concerning U.S. Persons, including who may receive such information and how it is handled. Recently approved minimization procedures are available on *IC on the Record*.[3]

Once the FISC approves the certifications, including the targeting and minimization procedures, the AG and the DNI can compel electronic communications service providers to assist in IC elements' collection against authorized Section 702 targets. A recent FISC opinion, dated November 2015, approving Section 702 certifications is available on *IC on the Record*.[4]

---

[2] These documents were posted on September 29, 2015 on *IC on the Record*. https://tmblr.co/ZZQjsq1vCrECI. The certification is available at https://www.dni.gov/files/documents/0928/DNI-AG%20702g%20Certification.pdf.

[3] The 2015 minimization procedures were posted on August 11, 2016. https://tmblr.co/ZZQjsq2Aa-Z92. The National Security Agency's (NSA's) procedures are available at https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.
CIA's procedures are available at https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf.
FBI's procedures are available at https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf.

[4] This FISC opinion ("November 2015 FISC opinion") was posted on April 19, 2016, https://tmblr.co/ZZQjsq25FiH2t, and is available at https://www.dni.gov/files/documents/20151106-

Why is FISA Section 702 necessary to protect national security?

Title VII of FISA is vital to keeping the nation safe. These authorities provide the government with a uniquely effective way to acquire information about the plans and identities of terrorists and terrorist organizations, including how they function and receive support. These authorities also enable collection of information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the U.S., and inform cybersecurity efforts. Losing these authorities would greatly impair the ability of the United States to respond to threats and to exploit important intelligence collection opportunities.

Some examples of the significant information collected through FISA Section 702 include:

- NSA has used collection authorized under FISA Section 702 to acquire extensive insight into the highest level decision-making of a Middle Eastern government. This reporting from Section 702 collection provided U.S. policymakers with the clearest picture of a regional conflict and, in many cases, directly informed U.S. engagement with the country. Section 702 collection provides NSA with sensitive internal policy discussions of foreign intelligence value.
- NSA has used collection authorized under FISA Section 702 to develop a body of knowledge regarding the proliferation of military communications equipment and sanctions evasion activity by a sanctions-restricted country. Additionally, Section 702 collection provided foreign intelligence information that was key to interdicting shipments of prohibited goods by the target country.
- Based on FISA Section 702 collection, CIA alerted a foreign partner to the presence within its borders of an al-Qaeda sympathizer. Our foreign partner investigated the individual and subsequently recruited him as a source. Since his recruitment, the individual has continued to work with the foreign partner against al-Qaeda and ISIS affiliates within the country.
- CIA has used FISA Section 702 collection to uncover details, including a photograph, that enabled an African partner to arrest two ISIS-affiliated militants who had traveled from Turkey and were connected to planning a specific and immediate threat against U.S. personnel and interests. Data recovered from the arrest enabled CIA to learn additional information about ISIS and uncovered actionable intelligence on an ISIS facilitation network and ISIS attack planning.
- NSA FISA Section 702 collection against an email address used by an al-Qaeda courier in Pakistan resulted in the acquisition of a communication sent to that address by an unknown individual located in the United States. The message indicated that the United States-based individual was urgently seeking advice regarding how to make explosives. The NSA passed this information to the FBI. Using a National Security Letter (NSL), the FBI was able to quickly identify the individual as Najibullah Zazi. Further investigation revealed that Zazi and a group of confederates had imminent plans to detonate explosives on subway lines in Manhattan. Zazi and his co-conspirators were arrested and pled guilty or were convicted of their roles in the planned attack. As the Privacy and Civil Liberties Oversight Board (PCLOB) found in its report, "[w]ithout the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded."

What are the privacy and civil liberties protections of FISA Section 702?

There are a number of provisions in the statute, the annual certifications and the targeting and minimization procedures that protect the privacy and civil liberties of U.S. persons and others located in the United States. Additionally, these provisions ensure that collection activities are focused on acquisition of specific types of information needed to protect national security.

- All acquisitions must be consistent with the Fourth Amendment.

- A significant purpose of any acquisition must be to obtain foreign intelligence information. No targeting may occur outside the scope of the specified foreign intelligence purpose of a certification.
- The government may not intentionally target a U.S. person anywhere in the world.
- The government may not intentionally target any person known at the time of acquisition to be in the United States, regardless of nationality.
- The government may not target someone located outside the United States for the purpose of targeting a particular, known person in this country or any U.S. person, regardless of location (often called "reverse targeting").
- The government may not target for acquisition "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States.
- Finally, Section 702 does not involve bulk collection and does not result in "mass" surveillance. The Government individually identifies or tasks each specific communications facility, such as a phone number or email address, based on an individualized assessment that it is used by a foreign intelligence target located abroad who communicates, possesses, or is likely to receive one of the categories of foreign intelligence information authorized for acquisition by the AG and DNI.

Section 702 requires that IC elements follow targeting and minimization procedures, which must be approved by the FISC, in effectuating Section 702 collection. As discussed in more detail above, the targeting procedures are designed to ensure that only foreign persons located abroad are targeted for foreign intelligence collection purposes. The minimization procedures are intended to protect any U.S. person information incidentally acquired in the course of collection activities.

Additionally, as further discussed below, the Department of Justice (DOJ), ODNI, the Judicial Branch, and Congress perform regular and rigorous approval and oversight of the IC's use of Section 702.

Finally, the IC itself is committed to furthering the principles of transparency—in FISA Section 702 and in other areas—as evidenced by the copious materials it has proactively declassified and provided to the public. For example, the IC and DOJ worked together to declassify and publicly release over 300 FISA-related documents, including many FISC opinions, to the maximum extent possible consistent with the need to protect classified sources, methods and techniques. This group also worked to make publicly available more than 5,000 additional pages, including IC-related official statements, congressional testimony, and transparency reporting. Many of these materials relate to the implementation of FISA Section 702.

Who oversees FISA Section 702?

The IC's use of FISA Section 702 is overseen by the FISC itself, ODNI, DOJ, Congress, and by internal IC element entities (such as Inspectors General and civil liberties protection officers). Additionally, certain formal entities, like the Privacy and Civil Liberties Oversight Board (PCLOB), may choose to further examine and make recommendations regarding FISA Section 702-related issues.

1. The Foreign Intelligence Surveillance Court (FISC)

Oversight of FISA Section 702 collection is conducted by the FISC, which reviews the government's Section 702 certifications, targeting procedures and minimization procedures for compliance with statutory and Fourth Amendment requirements. The intelligence agencies, via the DOJ's National Security Division (NSD) and with notice to ODNI, regularly report to the FISC any incidents of noncompliance with those targeting and minimization procedures.[5] (In 2015, ODNI publicly released certain letters notifying the FISC of incidents of

[5] The FISC Orders approving Section 702 activities require the government to adhere to the FISC Rules of Procedure, which include Rule 13 "Correction of Misstatement or Omission; Disclosure of Non-Compliance." These FISC Rules of Procedure are available at http://www.fisc.uscourts.gov/rules-procedure.

noncompliance, available on *IC on the Record*.[6]) The FISC takes those incident reports into consideration when making determinations on any subsequent certifications and targeting and minimization procedures submitted by the government.

2. ODNI and DOJ

The statute requires ODNI and DOJ oversight of FISA Section 702 activities. Agencies using Section 702 authority must report any potential incidents of noncompliance promptly to DOJ and ODNI. At least once every 60 days, NSD and ODNI conduct oversight of the agencies' activities under Section 702. These reviews are normally conducted on-site by a joint team from NSD and ODNI. The team evaluates and, where appropriate, investigates each potential incident of noncompliance and conducts a detailed review of agencies' targeting and minimization decisions. DOJ reports any identified incidents of noncompliance to the FISC. A summary of DOJ and ODNI's oversight of Section 702 activities that was submitted to the FISC as part of the 2015 certification application is available on *IC on the Record*.[7] An additional description of this oversight process is included in FISA Section 702 reports referred to as "Joint Assessments" (discussed below).

3. Congress

In addition to the Intelligence and Judiciary Committees' oversight of Section 702 activities, Congress receives regular reports, mandated by statute, describing IC elements' use of FISA-based collection authorities and any instances of noncompliance. The statute requires the AG and the DNI to report twice per year to the Intelligence and Judiciary Committees certain information concerning the implementation of Title VII. In particular, the statute requires the AG and the DNI to assess compliance with certain procedures and guidelines issued pursuant to FISA Section 702, reports referred to as "Joint Assessments." These Joint Assessments discuss trends in compliance and may include recommended changes to help reduce compliance incidents. Several of these past reports are available on IC on the Record.[8] In addition, the statute requires the AG to report twice per year on every incident of noncompliance relating to Section 702 that occurred during the applicable reporting period, requires certain Inspector Generals and certain heads of agencies to report on compliance with Section 702, and requires that Congress receive copies of the Section 702 certifications submitted to the FISC and copies of certain significant FISC opinions and related pleadings. Finally, FISA requires declassification review and public release of certain FISC opinions related to Section 702 and the public reporting of certain statistics related to the government's use of Section 702.

4. IC Element Internal Oversight

Components in the intelligence agencies themselves carry out oversight of activities conducted under Section 702. For instance, Section 702 requires that each Section 702 certification be supported, as appropriate, by one or more senior IC officials, such as the head of an IC element involved in implementing Section 702. This ensures such officials' regular involvement in the program. Moreover, all IC personnel who work with Section 702-acquired information must be trained on their agencies' Section 702 minimization procedures,

---

[6] These letters were posted on *IC on the Record* on September 29, 2015, https://tmblr.co/ZZQjsq1vCrECI. Two samples are available at https://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Walton%2018%20March%202014.pdf and https://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Hogan%2030%20July%202014.pdf.

[7] This oversight summary was posted on *IC on the Record* on August 11, 2016, https://tmblr.co/ZZQjsq2Aa_hL0, and is available at https://www.dni.gov/files/documents/UnclassOversightSummary.pdf.

[8] The most recent publicly released joint assessments were posted on *IC on the Record* on January 13, 2017, https://tmblr.co/ZZQjsq2H73g3F, and are available at https://icontherecord.tumblr.com/post/155810963663/release-of-joint-assessments-of-section-702.

and are also trained on how to report potential compliance issues to their agency's respective FISA program managers and other offices with oversight responsibilities. Additionally, internal bodies at the IC elements involved in implementing Section 702, such as compliance officers, civil liberties and privacy officers and inspectors general, have been involved in monitoring their agencies' compliance with FISA and the Section 702 targeting and minimization procedures. This reflects a multi-layered approach that builds U.S. person privacy protections into the design and operation of use of this authority. As with any healthy compliance program, there is a persistent, dedicated effort to reduce the occurrence of incidents, identify incidents or risks of incidents at the earliest possible moment, and implement mitigation measures wherever possible.

5. The Privacy and Civil Liberties Oversight Board (PCLOB)

In 2014, following an extensive review, the PCLOB issued a comprehensive and public report on Section 702 that addressed certain privacy concerns, ultimately concluding that the government's Section 702 program operates within legal constraints, collects valuable information and is both well-managed and effective in protecting national security.[9] The PCLOB specifically noted that, "To date, there are no known instances in which government personnel deliberately violated the statute, targeting procedures, or minimization procedures."[10]

In that report, the PCLOB made a number of recommendations to the government intended to enhance safeguards for privacy and civil liberties in the Section 702 program. In February 2016, the PCLOB reported that all of its recommendations had been implemented in full or in part by the government.[11]

---

[9] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (Jul. 2, 2014), https://www.pclob.gov/library/702-Report.pdf. The PCLOB recommendations were:

- NSA's targeting procedures should require written statements regarding the expected foreign intelligence value of collection against particular targets (Recommendation 1);
- FBI's minimization procedures should more clearly reflect FBI's U.S. person querying practices (Recommendation 2);
- Additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non-foreign intelligence criminal matters (Recommendation 2);
- NSA and CIA queries of Section 702 information using U.S. person query terms (*i.e.*, identifiers) should be accompanied by a written explanation of the reasonable likelihood the query will return foreign intelligence (Recommendation 3);
- A random sampling of tasking sheets, as well as NSA and CIA U.S. person query terms, should be submitted annually to the FISC to assist in the FISC's consideration of the FISA Section 702 certification renewals (Recommendation 4);
- Any rules governing the conduct of the Section 702 program should be incorporated into the annual certification process to the extent the FISC agrees that those rules are mandatory (Recommendation 5);
- NSA should continue to periodically assess the availability of additional or more advanced filtering techniques for "upstream" and for "about" collection (Recommendations 6 and 7);
- The government should publicly release the current Section 702 minimization procedures used by the CIA, FBI and NSA (Recommendation 8);
- The government should work to develop metrics for Congress and for public release providing additional insight about the extent to which NSA acquires and uses the U.S. persons information incidentally acquired through the Section 702 program (Recommendation 9); and
- The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs (Recommendation 10).

[10] *Id.* at 87-88 fn. 403.

[11] PCLOB, *Recommendations Assessment Report* 1 (Feb. 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

What makes FISA Section 702 constitutional?

Congress recognized the constitutionality of Section 702 when it reauthorized the FAA in 2012. Further, federal courts have consistently upheld the constitutionality of Section 702. For example, in *United States v. Mohamud*, (9th Cir. Dec. 5, 2016), the court unanimously held that no warrant is required for a search targeted at a foreign person abroad, who lacks Fourth Amendment rights, even though some U.S. person communications were incidentally acquired in that collection. The court found that Section 702 collection was reasonable under the Fourth Amendment's reasonableness balancing test, and that the targeting and minimization procedures sufficiently protected the defendant's privacy interests.

What are the other components of the FAA that are due to expire?

While this paper focuses principally on Section 702, other FAA provisions also provide critical intelligence tools and civil liberties and privacy protections. Prior to the enactment of the FAA, certain of these activities fell outside the scope of FISA and were governed by Section 2.5 of Executive Order 12333, but with FAA enactment, these activities were brought within the FISC's jurisdiction.

In contrast to Section 702, which focuses on foreign targets, Section 704 provides additional protection for collection activities directed against U.S. persons located outside of the United States. Section 2.5 of Executive Order 12333 requires the AG to approve the use of "any technique for which a warrant would be required if undertaken for law enforcement purposes" against U.S. persons abroad for intelligence purposes. The AG's approval must be based on a determination that probable cause exists to believe the U.S. person is a foreign power or an agent of a foreign power. Section 704 builds upon these pre-FAA requirements and provides that, in addition to the AG's approval, the government must obtain an order from the FISC in situations where the U.S. person target has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." The FISC order must be based upon a finding that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and that the target is reasonably believed to be located outside the United States. By requiring the approval of the FISC in addition to the approval of the AG, Section 704 provides an additional layer of civil liberties and privacy protection for U.S. persons located abroad.

In addition to Sections 702 and 704, the FAA added several other provisions to FISA. Section 701 provides definitions for Title VII. Section 703 allows the FISC to authorize an application targeting a U.S. person located outside the U.S. when the collection is conducted inside the United States. Like Section 704, Section 703 requires a finding by the FISC that there is probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably believed to be located outside the United States. Section 705 allows the government to obtain various authorities targeting U.S. persons simultaneously, provided that the requisite probable cause standard is met. Section 706 governs the use of Title VII-derived information in litigation; as with Traditional FISA, it requires the government to give notice to aggrieved persons when the government intends to use evidence obtained or derived from Title VII collection in legal proceedings. Section 707 provides for congressional oversight. Finally, Section 708 clarifies that nothing in the FAA is intended to limit the government's ability to obtain authorizations under other parts of FISA.

What FISA Section 702 issues are likely to arise in the re-authorization discussion?

1. Amount of U.S. Person Information Incidentally Acquired under Section 702

As described above, in enacting the FAA, Congress required minimization procedures to protect the privacy of U.S. person information acquired pursuant to Section 702. Some members of Congress and others have

requested that the DNI and NSA provide a public estimate of the number of U.S. person communications incidentally acquired under Section 702. The IC and DOJ have met with staff members of both the House and Senate Intelligence and Judiciary Committees, the PCLOB, and advocacy groups to explain the obstacles that hinder the government's ability to count with any accuracy or to even provide a reliable estimate of the number of incidental U.S. person communications collected through Section 702. For example, communicants do not usually self-identify or indicate their citizenship when communicating with the target. However, the IC recognizes the valid desire to have some sense of the nature of acquisition of incidental U.S. person communications and is working to produce a relevant metric that will inform the reauthorization debate.

2. Queries of Raw FISA Section 702 Data Using U.S. Person Identifiers

The government's minimization procedures restrict the ability of analysts to query the databases that hold "raw" Section 702 information *(i.e.*, where information identifying a U.S. person has not yet been minimized for permanent retention) using an identifier, such as a name or telephone number, that is associated with a U.S. person. Generally, queries of raw content are only permitted if they are reasonably designed to identify foreign intelligence information, although the FBI also may conduct such queries to identify evidence of a crime. As part of Section 702's extensive oversight, DOJ and ODNI review the agencies' U.S. person queries of content to ensure the query satisfies the legal standard. Any compliance incidents are reported to Congress and the FISC.

Querying databases containing Section 702 information does not result in any new acquisition of data; it is instead only an examination or re-examination of previously acquired information. Therefore, those queries are not separate "searches" for Fourth Amendment purposes.[12] The IC queries its databases to more quickly and efficiently sort and identify communications already lawfully collected, such as information potentially related to a terrorist plot against the United States, without having to sift through each individual communication that has been collected. For example, a query made by the IC is similar to a person searching an email inbox for a particular message: An analyst could try to read every message to find the one he or she is seeking, or—instead—could query the inbox to find a particular item or to quickly ascertain that the item is not present. Queries using U.S. person identifiers in Section 702 collection help the IC detect and evaluate connections between U.S. persons and lawfully targeted foreign persons involved in perpetrating terrorist attacks or other serious national security threats. Further, these queries can assist the IC in identifying situations where a U.S. person may be the subject of an imminent threat, with the goal of protecting the U.S. person from harm. Of note, several federal courts, including the FISC, have considered this issue and have concluded that queries using U.S. person identifiers are lawful.[13] Some have questioned whether a warrant requirement should be imposed, so that the IC would need to obtain a warrant before using a U.S. person identifier to query raw Section 702 collection. Adding such a requirement would severely hamper the speed and efficiency of operations by creating an unnecessary barrier to national security professionals' ability to identify potential threat information already in the lawful possession of the IC.

3. Upstream Collection

For most Section 702 collection, the government acquires data from the company providing the electronic communication service to the user. Some of NSA's Section 702 collection, however, has been obtained via "upstream" collection, in which the NSA obtains communications directly from the Internet backbone, with

[12] Queries of Section 702 data using U.S. person identifiers are sometimes mischaracterized in the public discourse as "backdoor searches."

[13] ***See, e.g.***, *November 2015 FISC opinion*, available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

the compelled assistance of companies that maintain those networks. In addition to collecting information via upstream that is "to" or "from" a target of Section 702 collection, NSA has also acquired information "about" targets of Section 702 – for example, where the target is neither the sender nor the recipient of the collected communication, but the target's tasked selector, such as an email address, is being passed between two other communicants. The FISC has considered upstream collection and concluded that it is lawful. Furthermore, this collection has allowed the IC to acquire unique intelligence that informs cybersecurity efforts.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu