Reauthorization of Title VII of the Foreign Intelligence Surveillance Act

March 17, 2023

Congressional Research Service
https://crsreports.congress.gov
R47477

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47477

March 17, 2023

Edward C. Liu
Legislative Attorney

Reauthorization of Title VII of the Foreign Intelligence Surveillance Act

Title VII of the Foreign Intelligence Surveillance Act (FISA) generally addresses electronic surveillance and other methods of acquiring foreign intelligence information that are directed at targets *outside* the United States. As a general matter, the principal effect of Title VII on FISA's legal framework is to apply FISA's protections to overseas targets dependent primarily on the target's nationality, and not the location where the acquisition occurs. Title VII includes separate provisions that authorize surveillance of both U.S. persons (Sections 703 and 704) and non-U.S. persons (Section 702), but it is the provisions related to non-U.S. persons that have garnered the most attention over the life of Title VII and during past reauthorization debates.

With respect to foreigners, Section 702 offers an alternative procedure for acquiring foreign intelligence information notwithstanding FISA's traditional requirements. Section 702 may only be used to target non-U.S. persons who are reasonably believed to be outside the United States in order to obtain foreign intelligence information. Unlike traditional FISA orders authorizing electronic surveillance, Section 702 does not require the Foreign Intelligence Surveillance Court (FISC) to make probable-cause determinations with respect to individual targets of surveillance or the facilities at which surveillance will be directed. Instead, Section 702 directs the Attorney General, in consultation with the Director of National Intelligence (DNI), to develop targeting procedures that intelligence officials will use to identify targets for surveillance under Section 702. As one federal court stated, "judicial review of Section 702 functions as a form of programmatic pre-clearance." The U.S. Courts of Appeals for the Second, Ninth, and Tenth Circuits have agreed that where "the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States, that target is not entitled to Fourth Amendment protections," even if the acquisition occurs in the United States.

For calendar year 2021, the Office of the DNI estimated that there were 232,432 non-U.S. persons targeted under Section 702.

Declassified FISC opinions from 2011 found that a type of electronic surveillance known as "about" collection (e.g., where the target email address is referenced in the body of an email to which the target is not a party) resulted in the estimated collection of "tens of thousands of wholly domestic communications each year" by the National Security Agency (NSA) due to technical limitations in how the government implemented such collection. The NSA announced in 2017 that it was no longer conducting "about" collection to prioritize "the greatest value to national security while reducing the likelihood that NSA will acquire communications of" persons who are not in contact with a foreign intelligence target. During the 2018 reauthorization of Title VII, Congress amended Section 702 to prohibit the resumption of "about" collection unless the Attorney General and DNI provide written notice of the intent to resume such collection to the House and Senate Judiciary and Intelligence Committees.

In 2018, Congress also amended Section 702 to require the Attorney General, in consultation with the DNI, to adopt querying procedures to govern how information collected under this Section is searched after it has been collected. Additionally, if the Federal Bureau of Investigation (FBI) seeks to query the contents of information acquired under Section 702 using a U.S. person identifier for a criminal investigation unrelated to national security, it must first obtain an order from the FISC supported by probable cause authorizing such query.

For calendar year 2021, the Office of the DNI reported that the NSA, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) used 8,790 U.S. person query terms to search Section 702 contents. CIA and NSA used 3,958 U.S. person query terms to search Section 702 metadata for the same period. FBI reports these statistics differently, counting the total number of *queries* using U.S. person terms, as opposed to CIA, NSA, and NCTC's practice of counting the number of U.S. person *terms* used. Between December 2020 and November 2021, FBI estimates it has conducted "fewer than 3,394,053" queries using a U.S. person term.

Title VII of FISA is scheduled to sunset on December 31, 2023.

Contents

Contacts

The Foreign Intelligence Surveillance Act (FISA) of 1978 provides a statutory mechanism by which the federal government may obtain a court order authorizing the use of electronic surveillance to collect foreign intelligence information.[1] In 2008, Congress enacted the FISA Amendments Act, which added a new Title VII to FISA to provide additional procedures for directing electronic surveillance or other types of intelligence collection at persons while they are located outside the United States.[2] Title VII of FISA is scheduled to sunset on December 31, 2023.[3]

Title VII of FISA generally addresses electronic surveillance and other methods of acquiring foreign intelligence information that target persons while they are outside the United States. With respect to overseas targets, Title VII includes provisions that authorize surveillance of U.S. persons while they are abroad (Sections 703 and 704).[4] The provisions of Title VII relating to non-U.S. persons (Section 702),[5] however, have garnered the most attention over the life of Title VII and in past reauthorization debates.

The main focus on Section 702 is likely due to its relatively more flexible requirements, compared to other federal statutory frameworks that authorize wiretapping. Since the late-1960s, a cornerstone of the American legal framework for government wiretapping has been the requirement that surveillance be authorized by a warrant or court order issued by a neutral and detached magistrate and accompanied by factual determinations about the particular target of surveillance that are supported by probable cause.[6] In contrast, surveillance under Section 702 does not require a court to make particular findings for each individual target of surveillance, although courts still play a role in Section 702 through the review and approval of procedures used by the government to identify individual surveillance targets and the access to and use of collected information.[7]

This CRS Report provides a brief summary of the original electronic surveillance authorities under Title I of FISA as they existed before 2008. It then explains the new procedures provided under Title VII and how they differ from electronic surveillance orders authorized under Title I of FISA (hereinafter referred to as "traditional FISA").

Traditional FISA

The Foreign Intelligence Surveillance Courts

From FISA's inception, a central feature of its framework is the use of specialized courts to hear applications for the use of FISA's investigative authorities and to issue orders authorizing the same. FISA establishes both a Foreign Intelligence Surveillance Court (FISC), which generally

[1] P.L. 95-511 (codified at 50 U.S.C. §§ 1801–1885c). In addition to court orders authorizing electronic surveillance, FISA also includes provisions to obtain court orders authorizing physical searches, 50 U.S.C. §§ 1821–1829; authorizing the installation of pen register or trap and trace devices (PR/TT), *id.* §§ 1841–1846; and compelling the production of certain categories of business records, *id.* §§ 1861–1864. For a high level summary of these authorities, *see* CRS In Focus IF11451, *Foreign Intelligence Surveillance Act (FISA): An Overview*, by Edward C. Liu.

[2] P.L. 110-261, § 101 (codified at 50 U.S.C. §§ 1881–1881g).

[3] *Id.* § 403(b) (as amended by P.L. 115-118, § 201(a)) (codified at 50 U.S.C. § 1881 note).

[4] 50 U.S.C. §§ 1881b, 1881c.

[5] *Id.* § 1881a.

[6] See CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[7] 50 U.S.C. § 1881a(j).

hears the government's *ex parte* applications to use FISA's investigative authorities, and a Foreign Intelligence Surveillance Court of Review (FISCR), which hears government appeals from the FISC.[8]

In 2015, Congress amended FISA to expressly authorize the presiding judges of the FISC and FISCR to jointly designate five individuals who are eligible to serve as an amicus curiae.[9] Each court may appoint an amicus curiae to assist with the review of any application or review that presents a novel or significant interpretation of the law.[10] In 2018, Congress included express authority for the FISC or FISCR to compensate appointed amici at a rate the court considers appropriate.[11] During the debate preceding the 2018 reauthorization, Congress also considered legislation to expand the scope of the amici's role before the FISC, including authorizing amici to make an application to the FISC or FISCR to refer a decision to the FISCR or the Supreme Court, respectively.[12]

Key FISA Definitions

FISA uses particular definitions of the terms "electronic surveillance," "U.S. person," and "agent of a foreign power." This section summarizes these key terms, which are important to understanding how Title VII's provisions differ from traditional FISA.

"Electronic Surveillance"

FISA's definition of "electronic surveillance" includes four categories.[13] Each category of electronic surveillance varies based on the target of the acquisition, the type of communication being acquired, and the location where the communication is being acquired. The four categories involve:

1. Acquisitions of wire or radio communications by targeting a specific U.S. person who is presently in the United States.
2. Acquisition of the contents of a wire communication to or from a person in the United States, if such acquisition occurs in the United States.
3. Acquisition of the contents of any radio communication where both the sender and all intended recipients are located within the United States.
4. Installation or use of an electronic, mechanical, or other surveillance device in the United States to acquire information, other than from a wire or radio communication.[14]

[8] *Id.* § 1803(a), (b). The FISC is comprised of eleven U.S. district court judges, designated by the Chief Justice of the U.S. Supreme Court, representing at least seven judicial circuits, three of whom must live within twenty miles of the District of Columbia. *Id.* § 1803(a)(1). The FISCR is comprised of three judges, also designated by the Chief Justice, and decisions of the FISCR may be reviewed by the Supreme Court. *Id.* § 1803(b). All members of the FISC and FISCR serve seven-year terms that expire on a rotating basis. *Id.* § 1803(d).

[9] *Id.* § 1803(i).

[10] *Id.* § 1803(i)(2).

[11] *Id.* § 1803(i)(11).

[12] *See, e.g.*, USA RIGHTS Act of 2017, S. 1997, 115th Cong. § 8 (2017).

[13] 50 U.S.C. § 1801(f).

[14] *Id.* § 1801(f)(1)–(4).

All four categories of electronic surveillance generally require some connection to the United States, requiring either the target or the acquisition to be in the United States. When the target is overseas, neither the first nor third category of electronic surveillance applies as they either require the target or all parties to the conversation to be within the United States. Conversely, the second and fourth categories of electronic surveillance may apply to an overseas target, but only if the acquisition occurs within the United States. As a result, acquisitions that neither take place within the United States nor target a person who is in the United States generally fall outside the scope of FISA's definition of electronic surveillance.

"U.S. Person"

FISA defines "U.S. person" to include both individuals and organizational entities.[15] With respect to individuals, a U.S. person includes U.S. citizens or aliens lawfully admitted for permanent residence.[16] As for organizations, FISA defines U.S. person to include corporations incorporated in the United States and unincorporated associations that have a substantial number of individual members who are U.S. citizens or lawfully admitted permanent residents.[17]

"Agent of a Foreign Power"

FISA's definition of "agent of a foreign power" has different elements depending on whether the agent is a U.S. person or a non-U.S. person. A non-U.S. person may be an agent of a foreign power if:

- The person acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism, irrespective of whether the person is inside the United States;
- The person acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the United States contrary to U.S. interests, when the circumstances show that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or
- The person engages in the international proliferation of weapons of mass destruction or activities in preparation therefor.

In contrast, any person (including a U.S. person) may be an agent of a foreign power if:

- The person knowingly engages in unlawful clandestine intelligence-gathering activities for or on behalf of a foreign power;
- The person, under the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
- The person knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power;

[15] *Id.* § 1801(i).

[16] *Id.*

[17] *Id.* The term "U.S. person" also excludes certain corporations or associations that fall under FISA's definition of a foreign power.

- The person knowingly aids or abets any person in, or conspires with any person to engage in, the conduct of activities described in the above; or
- The person knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power.

FISA Applications for Electronic Surveillance

Under Title I of FISA, the government may apply to the FISC for an order authorizing the government to conduct electronic surveillance against a particular target.[18] The government must include information in its application about, among other things, the identity of the target, the applicant's reasons for believing that the target is a foreign power or an agent of a foreign power, and that the facilities at which surveillance will be directed are being used, or are about to be used, by a foreign power or agent of a foreign power.[19]

Title I of FISA also requires the Attorney General to adopt procedures to minimize the acquisition and retention and prohibit the dissemination of nonpublic information of nonconsenting U.S. persons, consistent with the need to obtain, produce, and disseminate foreign intelligence information.[20] In particular, the minimization procedures must prohibit the dissemination of nonpublic information that would identify a U.S. person, unless such person's identity is necessary to understand foreign intelligence information or assess its importance.[21] The minimization procedures may allow the retention of information that is evidence of a crime and the dissemination of such information for law enforcement purposes.[22]

If the FISC finds that probable cause exists to support the application's determinations, it shall issue an order authorizing electronic surveillance for up to 90 days if the target is a U.S. person, up to 120 days if the target is a non-U.S. person, or up to one year if the target is a foreign government, a faction of a foreign nation, or an entity openly directed or controlled by a foreign government.[23] At the end of the order's duration, the FISC may grant extensions, which may be for up to one year if the target is not a U.S. person.[24]

FISA's Place in American Federal Wiretapping Law

FISA is one of several federal laws that govern the use of electronic surveillance for legitimate investigative purposes. The principal others are the U.S. Constitution's Fourth Amendment,[25] the

[18] *Id.* § 1804.

[19] *Id.* § 1804(a)(2), (3). FISA's definition of a "foreign power" generally includes foreign governments as well as factions of a foreign nation or nations; entities that are openly controlled by a foreign government; groups engaged in international terrorism, foreign-based political organizations; and entities engaged in the international proliferation of weapons of mass destruction, provided that such faction, entity, or group is not substantially composed of U.S. persons. *Id.* § 1801(a).

[20] *Id.* §§ 1801(h), 1804(a)(4).

[21] *Id.* § 1801(h)(2).

[22] *Id.* § 1801(h)(3).

[23] *Id.* § 1805(d)(1).

[24] *Id.* § 1805(d)(2).

[25] U.S. CONST. amend. IV.

Electronic Communications Privacy Act (ECPA),[26] and Executive Orders 12333[27] and 14086.[28] Each of these, and how they may overlap or interact with FISA, are discussed briefly below before examining Title VII's provisions in detail.

Fourth Amendment

The Constitution's Fourth Amendment provides a right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[29] In domestic criminal law investigations, "reasonableness" generally requires law enforcement officers to obtain a court-issued warrant before conducting a search,[30] but courts have recognized exceptions to the warrant requirement.[31] When the warrant requirement does not apply, government activity is generally subject to a "reasonableness" test under the Fourth Amendment.[32]

Government action constitutes a search when it intrudes upon a person's "reasonable expectation of privacy," which requires both that an individual "seeks to preserve something as private" and this subjective expectation of privacy is one that "society is prepared to recognize as reasonable."[33] As a general rule, the Fourth Amendment requires the government to show "probable cause" and obtain a warrant issued by a "neutral and detached magistrate" before conducting a search.[34] The U.S. Supreme Court first held that the recording or interception of electronic communications by law enforcement constitutes a search for purposes of the Fourth Amendment in its 1967 decision in *Katz v. United States*.[35] Since then, lower courts have similarly applied Fourth Amendment protections to the contents of email communications.[36] In 2018, the Supreme Court held that law enforcement's collection of seven days of a customer's historical location information from his cellular telephone provider constituted a Fourth Amendment search.[37]

The Supreme Court has not expressly addressed whether the warrant requirement categorically applies to the government's collection of foreign intelligence. In a 1972 case, the Supreme Court held that warrantless electronic surveillance for purposes of domestic intelligence gathering violated the Fourth Amendment, despite the government's assertion of a national security rationale.[38] The Court indicated that its conclusion might have been different, however, if the case

[26] 18 U.S.C. §§ 2510–2522.

[27] Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), as amended by Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004); Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

[28] Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 14, 2022).

[29] U.S. CONST. amend. IV.

[30] Lange v. California, 141 S. Ct. 2011, 2017 (2021).

[31] *Id.*

[32] *Id.* (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (stating "the ultimate touchstone of the Fourth Amendment is 'reasonableness'")).

[33] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (internal quotations omitted).

[34] *Id.*; *see also* Riley v. California, 573 U.S. 373, 382 (2014) ("[A] warrant ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." (internal quotations omitted)).

[35] Katz v. United States, 389 U.S. 347, 353 (1967), *overruling* Olmstead v. United States, 277 U.S. 438 (1928).

[36] *E.g.*, United States v. Warshak, 631 F.3d 266 (10th Cir. 2010).

[37] *Carpenter*, 138 S. Ct. at 2217.

[38] United States v. U.S. Dist. Ct. (*Keith*), 407 U.S. 297, 321–24 (1972).

had involved the electronic surveillance of foreign powers or their agents, within or outside the United States.[39]

The Supreme Court has also held that the Fourth Amendment (and, in particular, its warrant requirement) does not apply extraterritorially.[40] In *United States v. Verdugo-Urquidez*, the Court held that the Fourth Amendment does not apply to extraterritorial actions by law enforcement, at least where the defendant is a citizen and resident of a foreign country with "no voluntary attachment to the United States" and the place searched was located abroad.[41] Lower courts have extended *Verdugo-Urquidez*'s holding to conclude that the Fourth Amendment's warrant requirement does not apply to the surveillance of United States citizens abroad.[42]

The Electronic Communications Privacy Act (ECPA)

Following *Katz v. United States*, Congress enacted a federal statute, now known as the Electronic Communications Privacy Act (ECPA),[43] which generally prohibits government wiretapping except where the government has obtained a court order supported by probable cause and authorizing such surveillance against the target.[44] Court orders under ECPA are available only when the government is investigating the commission of certain *predicate* offenses specifically listed in the statute.[45] In some cases, the use of surveillance activities for foreign intelligence purposes might fall within the scope of the activities prohibited by ECPA. There are two exceptions to ECPA's general prohibitions that address this situation.

First, if the activity falls within FISA's definition of electronic surveillance, then it is not prohibited by ECPA if the government complies with FISA's procedures.[46] For example, the government could lawfully intercept a domestic phone call, which falls under FISA's definition of electronic surveillance, using FISA's traditional procedures even though ECPA generally prohibits such wiretapping.

Second, if that activity does not qualify as electronic surveillance, as that term is defined in FISA, but involves the acquisition of foreign intelligence information from international or foreign communications, then it is not subject to ECPA.[47] For example, the interception of an international telephone call would not be considered electronic surveillance for purposes of FISA if the target were the person on the non-domestic end of the conversation and the acquisition did

[39] *Id.* at 321–22. *See also In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the United States qualifies for the "special needs" exception to the warrant requirement).

[40] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[41] *Id.* at 274–75.

[42] *See In re* Terrorist Bombings, 552 F.3d 157, 171 (2d Cir. 2008); *see also* United States v. Zakharov, 468 F.3d 1171, 1179 (9th Cir. 2006) ("[T]he Fourth Amendment does not apply to searches and seizures by the United States against a non-resident alien in a foreign country.").

[43] 18 U.S.C. §§ 2510–2522.

[44] *Id.* § 2518.

[45] *Id.* § 2516(1).

[46] *Id.* § 2511(2)(e) (providing "it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act").

[47] *Id.* § 2511(2)(f). (explicitly disavowing any application of ECPA to the United States' acquisition of foreign intelligence information from international or foreign communications through a means other than electronic surveillance, as that term is defined in FISA).

not occur on United States soil. So long as the purpose of that acquisition was to acquire foreign intelligence information, then it would not be subject to ECPA's general prohibitions.

Although both exceptions result in the non-application of ECPA, they differ in one important aspect that is particularly relevant to understanding how Title VII altered FISA. Both ECPA and FISA provide that the two statutes constitute the exclusive means of conducting electronic surveillance, as defined in FISA.[48] As a result, using the procedures under FISA is compulsory for those activities that qualify as electronic surveillance but cannot be accomplished by ECPA. For example, if the government wishes to pursue electronic surveillance for foreign intelligence purposes that do not relate to a predicate offense required under ECPA, the government must generally comply with FISA. In contrast, before the FISA Amendments Act, the government was not required to use FISA's procedures for wiretapping activities that did not qualify as electronic surveillance, and which were also exempt from ECPA's general prohibition on wiretapping because they involved the collection of foreign intelligence information from international or foreign communications.[49]

Executive Orders 12333 and 14086

Issued in 1981, Executive Order 12333 addresses all U.S. foreign intelligence surveillance activities, including those which may fall outside of FISA's statutory scheme, such as activities conducted overseas targeting non-U.S. persons.[50] Section 2.5 of Executive Order 12333,[51] as amended,[52] delegates to the Attorney General the power to approve the use of any technique for intelligence purposes within the United States or against a U.S. person abroad. If a warrant would be required for law enforcement purposes, the executive order requires the Attorney General to determine in each case there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.[53] The authority delegated by Executive Order 12333 must be exercised in accordance with FISA, but also extends to activities beyond FISA's reach.

In 2022, President Joe Biden issued Executive Order 14086, "Enhancing Safeguards for United States Signals Intelligence Activities."[54] Executive Order 14086 imposes limits on the conduct of signals intelligence collection by executive agencies, and also includes a redress mechanism

[48] 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1812(a).

[49] PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 107 n.471 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf [hereinafter PCLOB REPORT] ("FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes.").

[50] *See Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page*, BRENNAN CTR. (Oct. 25, 2018), https://www.brennancenter.org/our-work/research-reports/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333.

[51] 46 Fed. Reg. 59,941 (Dec. 4, 1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004); Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

[52] 50 U.S.C. § 401 note.

[53] Exec. Order No. 12,333, § 2.5.

[54] Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 14, 2022).

under which individuals may seek review of alleged violations of, among other things, the Constitution, FISA, or Executive Orders 12333 or 14086.

Executive Order 14086 obliges executive agencies to conduct signals intelligence activities only in pursuit of "legitimate objectives," such as understanding or assessing the capabilities, intentions, or activities of a foreign government; protecting against terrorism, espionage, cybersecurity threats, or the development of weapons of mass destruction; or protecting the integrity of elections, political processes, and United States infrastructure from foreign governments.[55] Executive Order 14086 expressly prohibits the use of signals intelligence to pursue the objectives of suppressing criticism or dissent; suppressing privacy interests; suppressing a right to legal counsel; or disadvantaging individuals based on ethnicity, race, gender, gender identity, sexual orientation, or religion.[56]

Executive Order 14086 also limits the use of "bulk" surveillance to a smaller subset of similarly enumerated permissible objectives, and only after a determination that the information cannot reasonably be obtained through targeted collection.[57] For purposes of this limitation, "bulk surveillance" is defined as the collection of large quantities of signals intelligence data that are acquired without the use of discriminants (for example, specific identifiers or selection terms).[58] Executive Order 14086 also includes provisions to limit the dissemination, retention, and access of or to personal data obtained through signals intelligence.[59]

Under the redress mechanism established by Section 3 of Executive Order 14086, individuals may submit complaints to the Civil Liberties Protection Officer within the Office of the Director of National Intelligence, who is directed to investigate and, as necessary, remediate complaints.[60] Executive Order 14086 also directs the Attorney General to establish a Data Protection Review Court (DPRC) to review the Officer's determinations upon the request of either the complainant or the executive agency.[61] Unlike the FISC and FISCR, the DPRC does not include federal judges, or even federal employees, but is instead comprised of data privacy and national security legal practitioners selected by the Attorney General.[62] The DPRC may also be assisted by a designated "special advocate" who shall, among other things, advocate on behalf of a complainant's interests.[63]

Title VII of FISA

As discussed above, acquisitions that neither take place within the United States nor target a person who is in the United States generally fall outside the scope of FISA's definition of electronic surveillance. For example, the targeting of an international communication of a person who is abroad through an acquisition that also occurs overseas is not the type of electronic surveillance covered under FISA. Conversely, targeting the communications of the same person

[55] *Id.* § 2(b)(i). The President may update the list of legitimate objectives and the Director of National Intelligence shall publicly release any such updates, unless the President determines that doing so would pose a risk to the United States' national security. *Id.* § 2(b)(i)(B).

[56] *Id.* § 2(b)(ii).

[57] *Id.* § 2(c)(ii).

[58] *Id.* § 4(b).

[59] *Id.* § 2(c)(iii).

[60] *Id.* § 3(c)(i).

[61] *Id.* § 3(d). *See also* 28 C.F.R. §§ 201.1–201.12.

[62] Exec. Order No. 14,086, § 3(d)(i)(A).

[63] *Id.* § 3(d)(i)(C).

through an acquisition that occurs within the United States is the type of electronic surveillance covered under FISA.

These divergent outcomes turn on the geographic location in which acquisition of the communication occurs, and are independent of the nationality of the target. Under FISA's traditional Title I electronic surveillance authorities, if a foreign intelligence acquisition constitutes electronic surveillance, the government is generally required to obtain a court order to specifically authorize surveillance of the target. Extending the example above, this means that the targeting of a U.S. person abroad would not require an electronic surveillance court order if the acquisition is overseas, while the targeting of a non-U.S. person abroad would require one when the acquisition is domestic. This disparity leads to varying privacy protections based solely on where the acquisition of the communication occurs rather than the nationality of the target.

As a general matter, the main effect of Title VII on FISA's legal framework is to apply FISA's protections to overseas targets dependent based on the target's nationality, and not the location where the acquisition occurs. Title VII accomplishes this end through three main changes:

- First, it creates a procedure for targeting non-U.S. persons abroad without individualized court orders, even if the acquisition occurs within the United States;[64]
- Second, it imposes a requirement to obtain an individualized court order when targeting U.S. persons abroad, even if the acquisition occurs abroad;[65] and
- Third, it provides procedures that can be used to obtain court orders authorizing the targeting of specific U.S. persons abroad for electronic surveillance, the acquisition of stored communications, and other means of acquiring foreign intelligence information.[66]

Each of these elements is discussed in the following sections.

Section 702: Targeting Non-U.S. Persons Abroad

Section 702 offers an alternative procedure for acquiring foreign intelligence information despite the requirements of Title I of FISA or ECPA. Section 702 may only be used to target non-U.S. persons who are reasonably believed to be outside the United States, for the purpose of obtaining foreign intelligence information.[67] Additionally, Section 702 permits only acquisitions of information from or with the assistance of an electronic communication service provider.[68]

Surveillance under Section 702 is subject to FISC supervision through the court's review of a certification submitted jointly by the Attorney General and the Director of National Intelligence (DNI). Except in exigent circumstances,[69] the government may not conduct acquisitions under Section 702 unless the FISC issues an order after finding that the certification complies with

[64] 50 U.S.C. § 1881a.

[65] *Id.* § 1881c(a)(2).

[66] *Id.* §§ 1881b, 1881c.

[67] *Id.* § 1881a(a), (b)(3).

[68] *Id.* § 1881a(h)(2)(A)(vi). As used in Section 702, the term "electronic communication service provider" includes communications providers (such as telephone, email, or internet service providers (ISPs)) as well as remote computing service providers that provide "computer storage or processing services" to the public. *Id.* § 1881(b)(4).

[69] *Id.* § 1881a(c)(2) (defining exigent circumstances to be situations in which "intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order").

statutory requirements. The key components of the certification reviewed by the FISC are the targeting procedures, minimization procedures, and querying procedures that the government intends to use to govern the selection of targets and the retention, dissemination, use, and querying of information collected under Section 702.[70]

Targeting Procedures

Unlike traditional FISA orders authorizing electronic surveillance, Section 702 does not require the FISC to make probable-cause determinations with respect to individual targets of surveillance or the facilities at which surveillance will be directed.[71] Instead, Section 702 directs the Attorney General, in consultation with the DNI, to develop targeting procedures that intelligence officials will use to identify targets for surveillance under Section 702.[72] As stated by one federal court, "judicial review of Section 702 functions as a form of programmatic pre-clearance."[73]

The FISC then reviews these targeting procedures to ensure they are reasonably designed to limit targets to persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of communications in which all parties are known to be in the United States.[74] Additionally, the government may not intentionally target any persons in the United States or U.S. persons who are abroad.[75] The government may also not engage in "reverse targeting," in which an overseas non-U.S. person is targeted with the purpose of targeting a particular, known person reasonably believed to be within the United States.[76]

For calendar year 2021, the Office of the DNI estimated that there were 232,432 non-U.S. persons targeted under Section 702.[77]

Directives

After identifying a target with the FISC-approved targeting procedures, the government may issue directives to electronic communication service providers requiring them to provide the government with "all information, facilities, or assistance" needed to conduct the surveillance in a manner that does not undermine its secrecy.[78] A 2014 report by the Privacy and Civil Liberties Oversight Board describes how the government has used Section 702 directives to implement *downstream* and *upstream* collection programs.[79] In downstream collection, the government

[70] *Id.* § 1881a(j)(1)(A).

[71] *Id.* § 1881a(h)(4), (j)(2).

[72] *Id.* § 1881a(d).

[73] United States v. Hasbajrami, 945 F.3d 641, 652–53 (2d Cir. 2019).

[74] 50 U.S.C. § 1881a(d)(1), (j)(2)(B).

[75] *Id.* § 1881a(b)(1), (3).

[76] *Id.* § 1881a(b)(2).

[77] ODNI, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNIY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES at 17 (Apr. 2022), https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf [hereinafter ODNI CY2021 REPORT].

[78] *Id.* § 1881a(i).

[79] *See* PCLOB REPORT, *supra* note 49, at 7 ("There are two types of Section 702 acquisition: what has been referred to as 'PRISM' collection and 'upstream' collection."); Press Release, NSA, NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/ [hereinafter *NSA Press Release*] ("Under Section 702, NSA collects internet communications in two ways: 'downstream' (previously referred to as PRISM) and 'upstream.'").

typically directs consumer-facing communications service providers—such as internet service providers (ISPs), telephone providers, or email providers—to provide all communications "to or from" a "selector" (e.g., an email address) associated with a Section 702 target.[80] Upstream collection similarly involves the collection of all communications "to or from" a selector, but the requests are directed at telecommunications "backbone" providers (i.e., companies that operate the long-distance, high-capacity internet cables that interconnect with ISPs' local networks).[81]

"About" Collection

On top of collecting communications "to or from" the selector of a particular target, upstream collection has at times included collection of internet communications "about" the selector (e.g., where the target email address is referenced in the body of an email to which the target is not a party).[82] Declassified FISC opinions from 2011 found that "about" collection resulted in the estimated collection of "tens of thousands of wholly domestic communications each year" by the National Security Agency (NSA) due to technical limitations in how the government implemented "about" collection.[83] Specifically, "about" collection was implemented by capturing larger transactions containing multiple discrete communications, in which the selector appeared somewhere in the larger transaction.[84]

Upon being notified of this over-collection, the FISC then evaluated whether the previously approved targeting procedures were no longer reasonable given the prohibition in Section 702 against intentionally acquiring communications in which the parties are all known to be in the United States.[85] The FISC first held that the NSA's acquisition of wholly domestic communications through "about" collection was intentional because the NSA knew its technological limitations prevented it from avoiding the over-collection.[86] However, the FISC noted that the statute only prohibited intentional collection of wholly domestic communications where the government *knew* the parties to a communication were all located in the United States.[87] The FISC further noted that, due to technological limitations involved with acquiring these multi-communication transactions, it would be impossible for NSA to know at the time it acquires the transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.[88] Thus, the court held that targeting procedures continued to be "reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States," even though NSA knew with certainty that its collection would result in the acquisition of wholly domestic communications.[89]

[80] PCLOB REPORT, *supra* note 49, at 7.

[81] *Id.*

[82] *Id.* at 37.

[83] Redacted, 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011).

[84] *Id.* at *14.

[85] *Id.* at *15–17.

[86] *Id.* at *15.

[87] *Id.* at *16.

[88] *Id.*

[89] *Id.* Despite finding the targeting procedures to satisfy statutory requirements, the FISC went on to find that the minimization procedures did not contain sufficient safeguards to protect wholly domestic communications.

The NSA later announced in 2017 that it was no longer conducting "about" collection in its upstream collection activities in order to "retain the upstream collection that provides the greatest value to national security while reducing the likelihood that NSA will acquire communications of" persons who are not in contact with a foreign intelligence target.[90] During the 2018 reauthorization of Title VII, some legislative proposals would have barred the use of "about" collection under Section 702.[91] Ultimately, Congress amended Section 702 to conditionally prohibit the resumption of "about" collection unless the Attorney General and DNI provide written notice of the intent to resume such collection to the House and Senate Judiciary and Intelligence Committees.[92] A declassified FISC opinion from 2018 indicates the court construed this limitation as applying the use of "about" collection in either upstream or downstream collection.[93]

Minimization Procedures

Section 702 uses the same definition of minimization procedures that FISA provides for traditional FISA electronic surveillance or physical searches.[94] Accordingly, such procedures must be adopted by the Attorney General and be reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning nonconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[95]

The same declassified FISC opinions addressing "about" collection discussed in the previous section also provide an example of how the minimization procedures operate.[96] For example, the procedures required the prompt destruction of a wholly domestic communication upon recognition unless the NSA Director makes a written determination that "the communication contains foreign intelligence information or evidence of a crime, or that it falls into another narrow exception permitting retention."[97] If a communication is a foreign communication that discusses or mentions a U.S. person, but contains no foreign intelligence, it must be destroyed as early as practical, but no later than five years from the Section 702 authorization's expiration.[98] Reports based on U.S. person communications may be disseminated only if the U.S. person's identity is deleted and replaced with a generic term or symbol.[99] In limited circumstances, such as where the U.S. person is engaged in international terrorism, the identity may be provided if required for the performance of official duties.[100]

---

[90] *NSA Press Release*, *supra* note 79.

[91] *See* USA Liberty Act of 2017, S. 2158, 115th Cong. § 103(a)(2) (2017); USA Liberty Act of 2017, H.R. 3989, 115th Cong. § 102(a)(2) (2017); USA RIGHTS Act, H.R. 4124, 115th Cong. § 4 (2017); USA RIGHTS Act of 2017, S. 1997, 115th Cong. § 4 (2017); Preventing Unconstitutional Collection Act, H.R. 2588, 115th Cong. § 2 (2017).

[92] 50 U.S.C. § 1881a(b)(5).

[93] Redacted, 402 F. Supp. 3d 45, 60 (FISA Ct. 2018) ("Here, the text of Section 702(b)(5) does not distinguish between upstream and downstream collection or otherwise refer to how acquisition is conducted."), *aff'd in part sub nom. In re* DNI/AG 702(h) Certifications 2018, 941 F.3d 547 (FISA Ct. Rev. 2019).

[94] 50 U.S.C. § 1881a(e)(1).

[95] *E.g.*, *id.* § 1801(h).

[96] Redacted, 2011 WL 10945618, at *17–28 (FISA Ct. Oct. 3, 2011).

[97] *Id.* at *17.

[98] *Id.* at *18.

[99] *Id.*

[100] *Id.*

Although the FISC found these proposed minimization procedures to be sufficient with respect to ordinary collection of communications "to" or "from" the target, the court found these procedures to be deficient with respect to multi-communication transactions obtained through "about" collection, mainly because they failed to make provision for the prompt identification and segregation of irrelevant communications.[101] As a result, communications that were potentially wholly domestic could be retained for up to five years, effectively maximizing the retention of such information inconsistent with FISA's mandate to minimize retention of U.S. person information.[102]

Following the FISC's determination of a Fourth Amendment violation, the government presented revised minimization procedures to the FISC, which the court approved on November 30, 2011.[103] The revised minimization procedures addressed the court's concerns by requiring the segregation of those communications most likely to involve unrelated or wholly domestic communications; requiring special handling and markings for communications that could not be segregated; and reducing the retention period of upstream collection from five to two years.[104]

Querying Procedures

In 2018, Congress amended Section 702 to require the Attorney General, in consultation with the DNI, to adopt querying procedures to govern how information collected under this Section is searched after it has been collected.[105] Such procedures must also include a technical procedure under which a record is kept of each U.S. person term used for a query.[106] If the Federal Bureau of Investigation (FBI) seeks to query the contents of information acquired under Section 702 using a U.S. person identifier for a criminal investigation unrelated to national security, it must first obtain an order from the FISC authorizing such query.[107] The court shall issue such an order if it determines that probable cause exists to believe the contents of communications sought would provide evidence of criminal activity; contraband, fruits of a crime, or other items illegally possessed by a third party; or property designed for use, intended for use, or used in committing a crime.[108] A court order for such a query is not required if the FBI determines there is a reasonable belief that such contents could help mitigate or eliminate a threat to life or serious bodily harm.[109] This court-order requirement does not apply to queries of Section 702 information by other agencies, or to queries by the FBI to obtain foreign intelligence information or to pursue investigations related to U.S. national security.[110] For calendar year 2021, the FBI reported no

[101] *Id.* at *20.

[102] *Id.*

[103] *Redacted*, 2011 WL 10947772, at *1 (FISA Ct. Nov. 30, 2011).

[104] *Id.* at *3–5.

[105] 50 U.S.C. § 1881a(f)(1).

[106] *Id.* § 1881a(f)(1)(B).

[107] *Id.* § 1881a(f)(2).

[108] *Id.* § 1881a(f)(2)(D).

[109] *Id.* § 1881a(f)(2)(E).

[110] *Id.* § 1881a(f)(2)(F). Other bills considered by Congress during the 115th Congress would have more broadly required court orders to query Section 702 information using U.S. person terms. *E.g.*, USA Rights Act, S. 1997, 115th Cong. § 2 (2017) (prohibiting any officer or employee of the United States from conducting U.S. person queries of Section 702 information except with a court order or in emergency circumstances); USA Liberty Act of 2017, S. 2158, 115th Cong. § 101(a)(2) (2017) (requiring a court order for queries of Section 702 information using U.S. person terms, except in emergencies).

such court orders obtained from the FISC, although compliance reviews identified four instances in which a court order appeared to be required.[111]

Where the court order requirement does not apply, the standards for performing queries of Section 702 information are governed by the querying procedures approved by the FISC. The DNI has publicly released declassified versions of the querying procedures for the FBI, Central Intelligence Agency (CIA), the National Counterterrorism Center (NCTC), and the NSA.[112] Under NSA's querying procedures, the use of a U.S. person query term to search the contents of acquired communications must generally be approved by the NSA Office of General Counsel, based on a statement of facts establishing that the term is "reasonably likely to retrieve foreign intelligence information."[113] NSA queries of metadata (i.e., non-content information) using a U.S. person query term similarly require a written statement, but are not subject to approval by the Office of General Counsel.[114] NCTC and CIA querying procedures both generally require a written statement of facts showing that a U.S. person query term is reasonably likely to retrieve foreign intelligence information for both content or metadata queries.[115]

With respect to the FBI, its querying procedures reiterate the statutory court order requirement for non-foreign intelligence, non-national security U.S. person queries.[116] For other U.S. person queries, FBI's querying procedures also require a written statement of facts showing that the query is reasonably likely to retrieve foreign intelligence information or evidence of a crime.[117] FBI queries of metadata using a U.S. person term do not require a similar written statement.[118]

All four agencies' querying procedures also require recordkeeping of each U.S. person query term used by the agency, including the identity of the personnel who conducted the query.[119] The agencies will maintain such records for at least five years in a manner to allow the National

---

[111] ODNI CY2021 REPORT, *supra* note 77, at 22.

[112] Attorney General William Barr, *Querying Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Sept. 16, 2019), https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_CIA%20Querying%20Procedures_10.19.2020.pdf [hereinafter *CIA Querying Procedures*]; Attorney General William Barr, *Querying Procedures Used by the National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Oct. 19, 2020), https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NCTC%20Querying%20Procedures_10.19.2020.pdf [hereinafter *NCTC Querying Procedures*]; Attorney General William Barr, *Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Oct. 19, 2020), https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Querying%20Procedures_10.19.2020.pdf [hereinafter *NSA Querying Procedures*]; Attorney General William Barr, *Querying Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* (Sept. 16, 2019), https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Querying%20Procedures_10.19.2020.pdf [hereinafter *FBI Querying Procedures*].

[113] *NSA Querying Procedures* § IV.A. Approved terms may be used to query Section 702 information for up to one year, at which point the approval must be renewed. *Id*.

[114] *Id.*

[115] *CIA Querying Procedures* § IV.A, B.2; *NCTC Querying Procedures* § IV.A, B.2.

[116] *FBI Querying Procedures* § IV.A.2.

[117] *Id.* § IV.A.3.

[118] *Id.* at n.4.

[119] *NSA Querying Procedures* § IV.B; *FBI Querying Procedures* § IV.B; *CIA Querying Procedures* § IV.B; *NCTC Querying Procedures* § IV.B.

Security Division of the Department of Justice and the Office of the DNI to conduct oversight to ensure compliance with these procedures.[120] A declassified 2019 opinion from the FISCR addressed a prior version of the FBI's minimization procedures, under which records of queries did not distinguish between those that used U.S. person terms and those that did not.[121] The court held that this conflicted with the statutory requirement that the querying procedures "include a technical procedure whereby a record is kept of each United States person query term."[122]

For calendar year 2021, the Office of the DNI reported that NSA, CIA, and NCTC used 8,790 U.S. person query terms to search Section 702 contents.[123] CIA and NSA used 3,958 U.S. person query terms to search Section 702 metadata for the same period.[124] FBI reports these statistics differently, counting the total number of *queries* using U.S. person terms, as opposed to CIA, NSA, and NCTC's practice of counting the number of U.S. person *terms* used.[125] Between December 2020 and November 2021, FBI estimates it has conducted "fewer than 3,394,053" queries using a U.S. person term.[126]

Constitutional Challenges

Several U.S. Courts of Appeals have issued opinions addressing constitutional challenges to Section 702.[127] These cases involve appeals from criminal defendants who have been notified by the government that incriminating evidence was gathered under Section 702.[128] Several of these defendants have moved to suppress such evidence, arguing it was gathered unconstitutionally. Typically, these cases evaluate Section 702 under the Fourth Amendment, but one case also addresses whether Section 702 violates Article III of the Constitution, which limits the jurisdiction of federal courts to deciding "cases" or "controversies."[129]

With respect to the Fourth Amendment, the defendants have mainly argued that Section 702 is constitutionally defective because of the lack of a traditional warrant supported by an individualized finding of probable cause. In response, the Second, Ninth, and Tenth Circuits have unanimously held that where "the target of Section 702 surveillance is a foreign national located abroad having no substantial connections with the United States, that target is not entitled to Fourth Amendment protections," even if the acquisition occurs in the United States.[130] The government was thus not required to obtain a warrant before conducting the surveillance that targeted a non-U.S. person located abroad.

---

[120] *NSA Querying Procedures* § IV.B.3; *FBI Querying Procedures* § IV.B.3, 4; *CIA Querying Procedures* § IV.B.4; *NCTC Querying Procedures* § IV.B.4.

[121] In re: DNI/AG 702(h) Certifications 2018 [redacted], 941 F.3d 547, 557 (FISA Ct. of Rev. 2019).

[122] *Id.* at 566-67 (quoting 50 U.S.C. § 1881a(f)(1)(B)).

[123] ODNI CY2021 REPORT, *supra* note 77, at 18-19.

[124] ODNI CY2021 REPORT, *supra* note 77, at 19.

[125] ODNI CY2021 REPORT, *supra* note 77, at 20.

[126] ODNI CY2021 REPORT, *supra* note 77, at 21.

[127] United States v. Hasbajrami, 945 F.3d 641, 670 (2d Cir. 2019); United States v. Mohamud, 843 F.3d 420, 424 (9th Cir. 2016); United States v. Muhtorov, 20 F.4th 558, 594 (10th Cir. 2021), *cert. denied*, 143 S. Ct. 246 (2022).

[128] 50 U.S.C. § 1881e (citing *id.* § 1806).

[129] U.S. CONST. art. III, § 2; *see* United States v. Morton Salt Co., 338 U.S. 632, 641–42 (1950) ("Federal judicial power itself extends only to adjudication of cases and controversies . . . .").

[130] *Muhtorov*, 20 F.4th at 594; *Mohamud*, 843 F.3d at 439 ("[W]hat matters here is the location of the target, and not where the government literally obtained the electronic data."); *Hasbajrami*, 945 F.3d at 662 ("[T]he Fourth Amendment does not apply extraterritorially to the surveillance of persons abroad.").

In *Muhtorov v. United States*, the Tenth Circuit also addressed the defendant's claims that Section 702 violates Article III of the Constitution. The defendant argued that Article III prohibits advisory opinions and requires that courts must adjudicate only "concrete legal issues, presented in actual cases, not abstractions."[131] While acknowledging that the FISC's role under Section 702 is different than traditional Article III adjudication, the Tenth Circuit concluded that the FISC is not issuing advisory opinions under Section 702 because it applies legal principles to facts, and its determinations are legally binding and not merely advisory.[132] The court held that the targeting, minimization, and querying procedures submitted by the government are "detailed factual submissions" that the court must measure against Section 702's requirements.[133] The courts' determinations are therefore "grounded in evidentiary submissions, not abstract and hypothetical questions."[134]

Sections 703 and 704: Targeting U.S. Persons Abroad

As discussed above, Title VII establishes separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States.[135] Sections 703 and 704, detailed below, address the targeting of U.S. persons abroad for electronic surveillance and other types of acquisitions.

Requirement for Court Order

Section 704(a)(2) prohibits the intelligence community from targeting a U.S. person who is reasonably believed to be abroad unless authorized by the FISC or another provision of FISA.[136] This prohibition applies only when the target has a reasonable expectation of privacy and a warrant would be required if the acquisition was conducted in the United States for law enforcement purposes.[137] Whether a "reasonable expectation of privacy" exists requires both that an individual "seeks to preserve something as private" and this subjective expectation of privacy is one that "society is prepared to recognize as reasonable."[138] Although such a determination is inherently dependent upon the particular circumstances of a given case, it is likely that activities like physical searches, voice and email wiretaps, or the collection of geolocation information conducted on foreign soil could require authorization from the FISC based on the target's "reasonable expectation of privacy."[139]

Scope of Acquisitions

Having made the procedures of FISA compulsory in many foreign intelligence acquisitions in which U.S. persons abroad are targeted, Sections 703 and 704 then each establish procedures to provide the requisite FISC orders authorizing such acquisitions. The procedures under Section 703 apply only to electronic surveillance or the acquisition of stored electronic communications

[131] Golden v. Zwickler, 394 U.S. 103, 108 (1969).

[132] *Muhtorov*, 20 F.4th at 608.

[133] *Id.*

[134] *Id.* at 609.

[135] P.L. 110-261, §101 (codified at 50 U.S.C. §§ 1881–1881g).

[136] 50 U.S.C. § 1881c(a)(2).

[137] *Id*.

[138] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (internal quotations omitted).

[139] *See supra* note 33–37, and accompanying text.

or data that would traditionally require an order under FISA. The procedures under Section 704 apply in all other situations where the target has a reasonable expectation of privacy and a warrant would be required if the acquisition was conducted in the United States for law enforcement purposes.[140] Because the requirements of Section 704 are less stringent than Section 703, the statute prohibits the use of the former when the procedures of the latter would apply.

Procedures

The judicial procedures under Sections 703 and 704 generally follow the same structure used by the procedures that already existed in FISA to obtain a court order authorizing electronic surveillance or physical searches of U.S. persons within the United States. The government must submit an application for surveillance that identifies the target and the facts and circumstances relied upon that would justify the belief that the target is a foreign power or an agent of a foreign power, which the FISC must find to be supported by probable cause.[141] Because Title VII is intended to address targets outside the United States, the court must also find probable cause to believe that this geographical limitation has been met.[142]

Both Sections 703 and 704 also authorize short-term acquisitions if the Attorney General reasonably determines that an emergency exists and there is insufficient time to obtain a court order.[143] Such emergency acquisitions must be followed up with a formal application within seven days.[144]

Comparison of Sections 703 and 704

Although they are similar, the procedures under Sections 703 and 704 are not identical. Less specificity is generally required of the information in the application submitted under Section 704. Section 704 also does not require a statement that the information sought cannot be obtained by normal investigative means. Section 704 also only requires the minimization procedures to address dissemination of acquired information.[145] In contrast, Section 703 requires the minimization procedures to address the acquisition and retention of information.

Comparison with Traditional FISA

In at least two important ways, the standard that must be met under Sections 703 and 704 before the FISC will issue an order authorizing an acquisition is less stringent than the standard that has been traditionally required under FISA (in those situations where the activity qualifies as electronic surveillance and is therefore subject to FISA).

First, FISA traditionally required an application to identify the facilities to be searched or subject to electronic surveillance, and to show that those facilities are being used, or are about to be used, by the target. Second, FISA traditionally permitted U.S. persons to be targeted only if they are also linked to international terrorism or clandestine intelligence activities.[146] Neither Section 703 nor Section 704 contains these requirements.

---

[140] *Id.*

[141] 50 U.S.C. §§ 1881b(b)–(c), 1881c(b)–(c).

[142] *Id.*

[143] *Id.* §§ 1881b(d), 1881c(d).

[144] *Id.*

[145] *Id.* § 1881c(c)(1)(C).

[146] *Id.* § 1801(b).

Because all electronic surveillance was subject to FISA's standards under prior law, and Section 703 only applies to stored data if FISA would have traditionally required an order, it may be fair to characterize Section 703 simply as a relaxation of FISA's requirements when the target is a U.S. person abroad. The situation is different when considering the effect of Section 704 on prior law. The general prohibition embodied in Section 704 requiring a court order supported by probable cause when targeting U.S. persons abroad expands the scope of FISA to areas that were previously beyond its scope. For example, targeting the international communications of a U.S. person located abroad was generally not considered electronic surveillance if the acquisition did not occur on U.S. soil. Therefore, while no court order would have been traditionally required under FISA, the addition of Section 704 brings that conduct within the statute's ambit.

Effect of Sunset

Title VII of FISA is scheduled to sunset on December 31, 2023.[147] The sunset provision also includes special "transition procedures" that would apply to orders authorizing surveillance activities under Title VII that are in effect on December 31, 2023,[148] and would permit the continued effect of such orders until their normal expiration dates.

Author Information

Edward C. Liu
Legislative Attorney

Disclaimer

[147] P.L. 110-261, § 403(b)(1), 122 Stat. 2474 (2008), *as amended by* P.L. 112-238, §2(a)(1), 126 Stat. 1631; P.L. 115-118, § 201(a)(1), 132 Stat. 19 (2018).

[148] P.L. 110-261, § 404(b), 122 Stat. 2474 (2008) (codified as amended at 50 U.S.C. § 1801 note).