Reauthorization of the FISA Amendments Act

Edward C. Liu
Legislative Attorney

April 8, 2013

Congressional Research Service
7-5700
www.crs.gov
R42725

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

On December 30, 2012, President Obama signed H.R. 5949, the Foreign Intelligence Surveillance Act (FISA) Amendments Act Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017.

Reauthorizations of expiring provisions of FISA have been an annual occurrence in Congress since 2009. Prior to 2012, the legislative debate and reauthorizations largely dealt with three amendments to FISA that are commonly linked to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Most recently, in 2011, these three provisions were extended until June 1, 2015. For a more detailed discussion of these three provisions, *see* CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

In contrast, the reauthorization debated and passed in 2012 deals with Title VII of FISA, as added by the FISA Amendments Act of 2008. Title VII is only tangentially related to the subjects of the previous years' debates in that they are amendments to the same statute. Therefore, the legislative activity in prior years should be conceptually separated from the current debate and legislation that would address the expiration of Title VII of FISA at the end of this year.

Title VII of FISA, as added by the FISA Amendments Act of 2008, created new separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States. While some provisions of Title VII could be characterized as relaxing FISA's traditional standards for electronic surveillance and access to stored communications, other provisions of Title VII have expanded FISA's scope to require judicial approval of activities, such as surveillance of U.S. persons on foreign soil, that were previously unregulated by the statute.

Upon enactment of Title VII, a number of organizations brought suit challenging newly enacted procedures for surveillance of non-U.S. persons reasonably believed to be abroad. The suit alleged that this authority violated the targets' Fourth Amendment rights, because it permitted acquisition of international communications without requiring an individualized court order supported by probable cause. However, on February 26, 2013, in *Clapper v. Amnesty International*, the United States Supreme Court dismissed the suit because the plaintiffs had not suffered a sufficiently concrete injury to have legal standing to challenge Title VII. Therefore, the Court did not decide the merits of the Fourth Amendment question.

Contents

Contacts

Reauthorizations of expiring provisions of the Foreign Intelligence Surveillance Act (FISA) have been an annual occurrence in Congress since 2009.[1] Prior to 2012, the legislative debate and reauthorizations largely dealt with three amendments to FISA that are commonly linked to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).[2] Most recently, in 2011, these three provisions were extended until June 1, 2015.[3] For a more detailed discussion of these three provisions, *see* CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

In contrast, the reauthorization debated and passed in 2012 deals with Title VII of FISA, as added by the FISA Amendments Act of 2008. Title VII is only tangentially related to the subjects of the previous years' debates in that it amends the same statute. Therefore, the legislative activity in prior years should be conceptually separated from the current debate and legislation that would address the expiration of Title VII of FISA at the end of this year. This report describes the changes that were made by the FISA Amendments Act within the context of the government's authority to conduct surveillance for foreign intelligence purposes.

On December 30, 2012, President Obama signed H.R. 5949, the FISA Amendments Act Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017.

Overview of FISA and Other Laws Governing Surveillance

The Foreign Intelligence Surveillance Act (FISA) provides a statutory framework by which government agencies may, when gathering foreign intelligence information,[4] obtain authorization to conduct wiretapping[5] or physical searches,[6] utilize pen registers and trap and trace devices,[7] or access specified business records and other tangible things.[8] Authorization for such activities is typically obtained via a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created by FISA to act as a neutral judicial decision maker in the context of activities authorized by the statute.

[1] Department of Defense Appropriations Act, P.L. 111-118, §1004 (2009); An Act to extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, P.L. 111-141 (2010); FISA Sunsets Extension Act of 2011, P.L. 112-3 (2011); PATRIOT Sunsets Extension Act of 2011, P.L. 112-14 (2011).

[2] P.L. 107-56. In reality, only two of these provisions (relating to roving wiretaps and access to business records) were part of the USA PATRIOT Act. The third provision (relating to lone-wolf terrorists) initially arose from the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458.

[3] P.L. 112-14.

[4] Although FISA is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes. For example, it extends to the collection of information necessary for the conduct of foreign affairs. *See* 50 U.S.C. §1801(e) (2008) (definition of "foreign intelligence information").

[5] 50 U.S.C. §§1801-1808.

[6] 50 U.S.C. §§1822-1826.

[7] 50 U.S.C. §§1841-1846. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular telephone line. *See* 18 U.S.C. §3127(3)-(4) (2008).

[8] 50 U.S.C. §§1861-1862 (2008).

Title VII, added by the FISA Amendments Act of 2008, provides additional procedures for the acquisition of foreign intelligence information regarding persons who are believed to be outside of the United States. These provisions affect both U.S. persons[9] as well as other non-U.S. persons. Specifically, the FISA Amendments Act added

- a new procedure for targeting non-U.S. persons abroad without individualized court orders;[10]
- a new requirement to obtain an individualized court order when targeting U.S. persons abroad;[11] and
- new procedures that can be used to obtain court orders authorizing the targeting of U.S. persons abroad for electronic surveillance, the acquisition of stored communications, and other means of acquiring foreign intelligence information.[12]

FISA is just one of several federal laws that govern the use of electronic surveillance for legitimate investigative purposes. The principal others are the Electronic Communications Privacy Act (ECPA), Executive Order 12333, and the Fourth Amendment. Each of these, and the manner in which they may overlap or interact with FISA, will be discussed briefly before turning to the provisions added by the FISA Amendments Act.

Electronic Communications Privacy Act (ECPA)

ECPA provides three sets of general prohibitions accompanied by judicially supervised exceptions to facilitate law enforcement investigations.[13] The prohibitions address (1) the interception of wire, oral, or electronic communications (wiretapping);[14] (2) access to the content of stored electronic communications and to communications transaction records;[15] and (3) the use of trap and trace devices and pen registers (essentially in-and-out secret "caller id" devices).[16]

In some circumstances, 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 in question falls within the definition of electronic surveillance under FISA, then it may be conducted if the government complies with FISA's procedures. For example, the

[9] A U.S. person is defined as a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. 50 U.S.C. §1801(i).

[10] 50 U.S.C. §1881a.

[11] 50 U.S.C. §1881c(a)(2).

[12] 50 U.S.C. §§1881b, 1881c.

[13] See CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle, for a more detailed discussion of the federal laws governing wiretapping and electronic eavesdropping, along with appendices including copies of the texts of ECPA and FISA.

[14] 18 U.S.C. §§2510-2522.

[15] 18 U.S.C. §§2701-2712.

[16] 18 U.S.C. §§3121-3127. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular telephone line. *See* 18 U.S.C. §3127(3)-(4).

interception of a domestic telephone call is the type of activity that would generally be prohibited by ECPA. It would also qualify as electronic surveillance under FISA. Therefore, if the government obtained a court order from the FISC authorizing the interception of that call, it would be a lawful surveillance activity notwithstanding the general prohibition against wiretapping found in ECPA.

Second, if the activity in question is not 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.[17] 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 would 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 the general prohibitions in ECPA.

Although both exceptions result in the non-application of ECPA, they differ in one important aspect that is particularly relevant to understanding the changes wrought by Title VII of FISA. Both ECPA and FISA provide that the two statutes constitute the exclusive means of conducting electronic surveillance, as defined in FISA.[18] As a result, using the procedures under FISA is compulsory for those activities that qualify as electronic surveillance but cannot be accomplished by, and are exempt from, ECPA. In contrast, prior to the FISA Amendments Act, FISA's procedures were generally never needed for wiretapping activities that did not qualify as electronic surveillance, and which were also exempt from ECPA because they involved international or foreign communications. However, as discussed below, the recently added Section 704 of FISA does make FISA's procedures compulsory when the target of such surveillance is a United States person. Those activities that remain beyond the scope of either ECPA or FISA are governed by Executive Order 12333 and the Fourth Amendment, discussed in the next two sections.

Executive Order 12333

Section 2.5 of Executive Order 12333,[19] as amended,[20] 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 that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated by Executive Order 12333 must be exercised in accordance with FISA, but also extends to activities beyond FISA's reach.

[17] 18 U.S.C. §2511(2)(f). (explicitly disavowing any application of ECPA to the acquisition by the United States of foreign intelligence information from international or foreign communications through a means other than electronic surveillance, as that term is defined in FISA.).

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

[19] 46 *Federal Register* 59,941 (December 4, 1981), as amended by E.O. 13284, 68 *Federal Register* 4,075 (January 23, 2003); E.O. 13355, 69 *Federal Register* 53,593 (August 27, 2004); and E.O. 13470, 73 *Federal Register* 45,325 (July 30, 2008).

[20] 50 U.S.C. §401 note.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution protects against "unreasonable searches and seizures."[21] In domestic criminal law investigations, it generally requires law enforcement officers to obtain a court-issued warrant before conducting a search.[22] When the warrant requirement does not apply, government activity is generally subject to a "reasonableness" test under the Fourth Amendment.[23]

The extent to which the warrant requirement applies to the government's collection of foreign intelligence is unclear. In a 1972 case, the Supreme Court invalidated warrantless electronic surveillance of domestic organizations on Fourth Amendment grounds, despite the government's assertion of a national security rationale.[24] However, it indicated that its conclusion might be different in a future case involving the electronic surveillance of foreign powers or their agents, within or outside the United States.[25] In a 2002 case, the Foreign Intelligence Surveillance Court of Review upheld FISA, as amended by the USA PATRIOT Act, against a Fourth Amendment challenge.[26] The court assumed, without deciding the question, that FISA court orders do not constitute warrants for purposes of the Fourth Amendment analysis. Relying on a general reasonableness analysis, it nonetheless upheld such orders, emphasizing both the privacy protections in the statutory framework and the governmental interest in preventing national security threats.[27]

Procedure for Targeting Non-U.S. Persons Abroad Without Individualized Court Orders Under Section 702

In late 2005, the *New York Times* reported that the federal government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[28] Subsequently, President George W. Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National

[21] U.S. Const. amend. IV.

[22] *See* Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process without prior approval by judge or magistrate are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.").

[23] Also called the "general balancing," "general reasonableness," or "totality-of-the circumstances" test, it requires a court to determine the constitutionality of a search or seizure "by assessing, on the one hand, the degree to which [a search or seizure] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Samson v. California, 547 U.S. 843, 848 (2006).

[24] U.S. v. U.S. District Court, 407 U.S. 297, 321-24 (1972) (also referred to as the *Keith* case, so named for the District Court judge who initially ordered disclosure of unlawful warrantless electronic surveillance to the defendants).

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

[26] In re Sealed Case, 310 F.3d 717 (Foreign Intell. Survellance Ct. Rev. 2002).

[27] *Id*. at 738-46.

[28] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, December 16, 2005, at 1.

Security Agency to conduct a Terrorist Surveillance Program (TSP) to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations" based upon his asserted "constitutional authority to conduct warrantless wartime electronic surveillance of the enemy."[29] Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to January of 2007.[30]

After the TSP activities were concluded in 2007, Congress enacted the Protect America Act (PAA), which established a mechanism for the acquisition, via a joint certification by the Director of National Intelligence (DNI) and the Attorney General (AG), but without an individualized court order, of foreign intelligence information concerning a person reasonably believed to be outside the United States.[31] This temporary authority ultimately expired after approximately six months, on February 16, 2008. Several months later, the Congress enacted the FISA Amendments Act of 2008, which created separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States under a new Title VII of FISA.[32] Section 702 provides procedures for targeting non-U.S. persons and is discussed in more detail below.

Scope of Acquisitions

Like its predecessor in the PAA, Section 702 permits the AG and the DNI to jointly authorize targeting of persons reasonably believed to be located outside the United States, but is limited to targeting non-U.S. persons. Once authorized, such acquisitions may last for periods of up to one year. Under subsection 702(b) of FISA, such an acquisition is also subject to several limitations. Specifically, an acquisition

- may not intentionally target any person known at the time of acquisition to be located in the United States;
- may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- may not intentionally target a U.S. person reasonably believed to be located outside the United States;
- may not intentionally acquire 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; and
- must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.[33]

[29] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, at 5, 17, January 19, 2006, http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf. *See also* CRS Report R40888, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea.

[30] S.Rept. 110-209, at 4. *See also* Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (January 17, 2007).

[31] P.L. 110-55, 50 U.S.C. §§1805a-1805c.

[32] P.L. 110-261, §101, 50 U.S.C. §§1881-1881g.

[33] 50 U.S.C. §1881a(b).

Acquisitions under Section 702 are also geared towards electronic communications or electronically stored information. This is because the certification supporting the acquisition, discussed in the next section, requires the AG and DNI to attest that, among other things, the acquisition involves obtaining information from or with the assistance of an electronic communication service provider.[34] This would appear to encompass acquisitions using methods such as wiretaps or intercepting digital communications, but may also include accessing stored communications or other data. Such a conclusion is also bolstered by the fact that the minimization procedures required to be developed under Section 702 reference the minimization standards applicable to physical searches under Title III of FISA.[35]

Certification Procedure

Section 702 requires the joint AG/DNI authorization to be predicated on either the existence of a court order approving of a joint certification submitted by the AG and DNI, or a determination by the two officials that exigent circumstances exist.

The certification is not required to identify the individuals at whom such acquisitions would be directed, but must attest, in part, that targeting procedures are in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the FISC that are reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[36] The applicable targeting and minimization procedures are subject to judicial review by the FISC, but the court is not required to look behind the assertions made in the certification.

Generally, if the certification and targeting and minimization procedures meet the statutory requirements and are consistent with the Fourth Amendment, a FISC order approving them will be issued prior to implementation of the acquisition of the communications at issue. If the FISC finds deficiencies in the certification, targeting procedures, or minimization procedures, the court shall issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any such deficiency within 30 days or cease, or not begin, the implementation of the authorization for which the certification was submitted.

Exigent Circumstances

In the absence of a court order described above, the AG and DNI may also authorize the targeting of persons reasonably believed to be non-U.S. persons abroad if they determine that exigent circumstances exist which would cause the loss or delay of important national security intelligence. A certification supporting such acquisition is required to be submitted to the FISC as soon as practicable, but no later than seven days after the determination of exigency has been

[34] 50 U.S.C. §1881a(g)(2)(A)(vi).

[35] 50 U.S.C. §1881a(e)(1) (referencing 50 U.S.C. §1821(4)).

[36] The certification must also attest that guidelines have been adopted to ensure that the specifically prohibited types of surveillance activities listed in §702(b), such as reverse targeting, are not conducted.

made.[37] Collection of information is permitted during the period before a certification is submitted to the FISC.

Comparison with Prior Law

As discussed above, surveillance activities that meet the definition of electronic surveillance in FISA must be authorized either under FISA or ECPA.[38] Prior to the enactment of Section 702, FISA only permitted sustained electronic surveillance or access to electronically stored communications after the issuance of a court order that was specific to the target. Since Section 702 does not require an individualized court order, the most dramatic effect of its enactment compared to the traditional provisions of FISA has been in those situations in which Section 702 encompasses activities that qualify as electronic surveillance.

FISA defines several different categories of electronic surveillance, but only two are relevant to Section 702.[39] The first is the acquisition, in the United States, of international wire communications, which are defined by FISA as communications where one endpoint of the captured communication is in the United States.[40] Consequently, Section 702 provides a mechanism for the domestic acquisition, without a court order, of communications that persons in the United States, including citizens, would be a party to. Prior to the enactment of Section 702, such acquisitions would require a court order in all but emergency situations.[41]

The second category of electronic surveillance to which Section 702 is applicable is the 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, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[42] Examples of such surveillance would include things such as hidden microphones and may also include access to stored communications.[43] Section 702 may also permit access to electronically stored communication that does not qualify as electronic surveillance through the use of physical searches, so long as the information is acquired from or with the assistance of an electronic communication service provider. As with interception of international wire communications, such examples of electronic surveillance or access to stored communications would likely have required an individualized court order under FISA as it existed prior to Section 702.

Legal Challenges

Upon enactment of Title VII, a number of organizations brought suit challenging the joint authorization procedure for surveillance of non-U.S. persons reasonably believed to be abroad.

---

[37] 50 U.S.C. §1881a(g)(1)(B).

[38] *See* discussion *supra* at "Electronic Communications Privacy Act (ECPA)."

[39] The irrelevant categories of electronic surveillance deal with situations in which the target of the surveillance is a U.S. person or present in the United States, both of which would disqualify the use of §702.

[40] 50 U.S.C. §1801(f)(2).

[41] *See* 50 U.S.C. §1805(e)(1).

[42] 50 U.S.C. §1801(f)(4).

[43] *See* David Kris and Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS §7:27 (2012) (discussing application of definition of electronic surveillance to stored e-mail and voice mail).

The suit alleged that this authority violated the Fourth Amendment's prohibition against unreasonable searches.[44] In order to establish legal standing to challenge Title VII, the plaintiffs had argued that the financial costs they incurred in order to avoid their reasonable fear of being subject to surveillance constituted a legally cognizable injury. However, on February 26, 2013, in *Clapper v. Amnesty International*, the United States Supreme Court held that the plaintiffs had not suffered a sufficiently concrete injury to have legal standing to challenge Title VII.[45] Because the Court had no jurisdiction to proceed to the merits of the plaintiffs' claims, it did not decide the Fourth Amendment question.

Procedures for Targeting U.S. Persons Abroad Using Court Orders Under Sections 703 and 704

As discussed above, the FISA Amendments Act created separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States.[46] Sections 703 and 704, discussed in more detail below, address the targeting of U.S. persons abroad for electronic surveillance and other types of acquisitions.

Requirement for Court Order

As an initial matter, 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.[47] This prohibition only applies in circumstances 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.[48] Whether a "reasonable expectation of privacy" exists depends upon whether an "individual manifested a subjective expectation of privacy in [a] searched object" and whether "society is willing to recognize that expectation as reasonable."[49] Although such a determination is inherently dependent upon the particular circumstances in a given case, it is likely that activities like physical searches and wiretaps conducted on foreign soil would require authorization from the FISC based on the target's "reasonable expectation of privacy."

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

[44] *But see* In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009-1016 (U.S. Foreign Intell. Surveil Ct. Rev. 2008) (upholding similar joint authorization procedure under the Protect America Act in the face of a Fourth Amendment challenge brought by telecommunications provider).

[45] Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013).

[46] P.L. 110-261, §101, 50 U.S.C. §§1881-1881g.

[47] 50 U.S.C. §1881c(a)(2).

[48] *Id*.

[49] Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing California v. Ciraolo, 476 U.S. 207, 211 (1986)).

703 apply only to electronic surveillance or the acquisition of stored electronic communications 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.[50] However, 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.[51] Because Title VII is intended to address targets that are outside of the United States, the court must also find that probable cause to believe that this geographical limitation has been met.[52]

Both Sections 703 and 704 also provide authority for short-term acquisitions if the AG reasonably determines that an emergency situation exists and there is insufficient time to obtain a court order.[53] Such emergency acquisitions must be followed up with a formal application within seven days.[54]

Comparison of Sections 703 and 704

Although they are similar, the procedures under Sections 703 and 704 are not identical to each other. 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.[55] In contrast, Section 703 also requires the minimization procedures to address the acquisition and retention of information.

Comparison with Prior Law

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.

First, FISA traditionally required an application to identify the facilities that will be searched or subject to electronic surveillance, and to demonstrate that those facilities are being used, or are

[50] *Id.*

[51] 50 U.S.C. §§1881b(b)-(c), 1881c(b)-(c).

[52] *Id.*

[53] 50 U.S.C. §§1881b(d), 1881c(d).

[54] *Id.*

[55] 50 U.S.C. §1881c(c)(1)(C).

about to be used, by the target. Second, FISA traditionally only permitted U.S. persons to be targeted if they are also linked to international terrorism or clandestine intelligence activities.[56] Neither of these is required under Section 703 or Section 704.

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.

However, 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 ambit of the statute.

Sunset

On December 30, 2012, President Obama signed H.R. 5949, the FISA Amendments Act Reauthorization Act of 2012, which extends Title VII of FISA until December 31, 2017. Absent intervening legislation, Title VII of FISA will be automatically repealed on that date.[57] Transition procedures would apply to orders authorizing surveillance activities pursuant to Title VII that are in effect on December 31, 2017,[58] and would permit the continued effect of such orders until their normal expiration dates.

Author Contact Information

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

[56] 50 U.S.C. §1801(b).

[57] 50 U.S.C. §1881 note.

[58] *Id.* at §404(b).