Congressional Research Service
Informing the legislative debate since 1914

Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)

(name redacted)
Legislative Attorney

April 13, 2016

Congressional Research Service
7-....
www.crs.gov
R44457

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

After the attacks of September 11, 2001, President George W. Bush authorized the National 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." After the TSP activities were concluded in 2007, Congress enacted the Protect America Act (PAA, P.L. 110-55), 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. This temporary authority ultimately expired after approximately six months, on February 16, 2008. Several months later, Congress enacted the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (P.L. 110-261), 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. Title VII of FISA was reauthorized in late 2012 (P.L. 112-238); this authority now sunsets on December 31, 2017.

Significant details about the use and implementation of Section 702 of Title VII, which provides procedures for targeting non-U.S. persons who are abroad, became known to the public following reports in the media beginning in summer 2013. According to a partially declassified 2011 opinion from the Foreign Intelligence Surveillance Court (FISC), the National Security Agency (NSA) collected 250 million Internet communications per year under Section 702. Of these communications, 91% were acquired "directly from Internet Service Providers," using a mechanism referred to as "PRISM collection." The other 9% were acquired through what NSA calls "upstream collection," meaning acquisition while Internet traffic is in transit from one unspecified location to another.

In 2015, Congress enacted the USA FREEDOM Act (P.L. 114-23) to reauthorize and amend various portions of FISA. While most of the amendments dealt with portions of FISA that were unrelated to Section 702, the act did include authority to continue surveillance of a non-U.S. person for 72 hours after the target is reasonably believed to be within the United States, but only if a lapse in surveillance of the target would pose a threat of death or serious bodily harm. A traditional FISA order for electronic surveillance must be obtained to continue surveillance after that period.

Contents

Contacts

Beginning 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."[1] Subsequently, President George W. Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National 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."[2] Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to January 2007.[3]

After the TSP activities were concluded in 2007, Congress enacted the Protect America Act (PAA, P.L. 110-55), 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.[4] This temporary authority ultimately expired after approximately six months, on February 16, 2008. Several months later, Congress enacted the Foreign Intelligence Surveillance Act (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.[5] Title VII of FISA was reauthorized in late 2012; this authority now sunsets on December 31, 2017.[6]

Significant details about the use and implementation of the Section 702 of Title VII, which provides procedures for targeting non-U.S. persons, became known to the public following reports in the media beginning in summer 2013.[7] According to a partially declassified 2011 opinion from the Foreign Intelligence Surveillance Court (FISC), the National Security Agency (NSA) collected 250 million Internet communications per year under Section 702.[8] Of these communications, 91% were acquired "directly from Internet Service Providers," using a mechanism referred to as "PRISM collection."[9] The other 9% were acquired through what NSA calls "upstream collection," meaning acquisition while Internet traffic is in transit from one unspecified location to another.[10]

---

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

[2] 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 (name redacted) and (name redacted) .

[3] 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).

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

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

[6] P.L. 112-238.

[7] *See, e.g.*, Siobhan Gorman, Even Perez, Janet Hook, *U.S. Collects Vast Data Trove*, WALL STREET JOURNAL, June 7, 2013, available at http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html.

[8] Foreign Intelligence Surveillance Court Memorandum Opinion, at 29 (FISA Ct. October 3, 2011) (Bates, J.) available at http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

[9] *Id.* at 29-30.

[10] *Id.* at 29, n.24.

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;[11]
- 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.[12]

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.[13] 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.[14]

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. Rather, the certification 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

[11] An amendment by the USA FREEDOM Act (P.L. 114-23 provides a limited authority to continue surveillance of a non-U.S. person for 72 hours after the target is reasonably believed to be in the United States, if a lapse in surveillance of the target poses a threat of death or serious bodily harm). 50 U.S.C. § 1805(f). A traditional FISA order for electronic surveillance must be obtained to continue surveillance after that period. *Id.*

[12] 50 U.S.C. § 1881a(b).

[13] 50 U.S.C. § 1881a(g)(2)(A)(vi).

[14] 50 U.S.C. § 1881a(e)(1) (referencing 50 U.S.C. § 1821(4)).

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.[15] The applicable targeting and minimization procedures are subject to judicial review by the FISC, but the court is not required to look beyond 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 will 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 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 made.[16] Collection of information is permitted during the period before a certification is submitted to the FISC.

In 2015, Congress included an amendment to FISA in the USA FREEDOM Act (P.L. 114-23), to facilitate the continued surveillance of a target that was believed to be abroad, but is later found to be within the United States. As noted above, Section 702 originally did not permit surveillance of persons reasonably believed to be in the United States at the time of acquisition. As amended by the USA FREEDOM Act, surveillance of a non-U.S. person may continue for 72 hours after the target is reasonably believed to be within the United States, if a lapse in surveillance of the target poses a threat of death or serious bodily harm.[17] A traditional FISA order for electronic surveillance must be obtained to continue surveillance after that period.[18]

Constitutional Challenges

Section 702 at the Supreme Court

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. The suit alleged that this authority violated the Fourth Amendment's prohibition against unreasonable searches.[19] 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

[15] 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. 50 U.S.C. § 1881a(g)(2)(A)(iii).

[16] 50 U.S.C. § 1881a(g)(1)(B).

[17] 50 U.S.C. § 1805(f).

[18] *Id.*

[19] *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).

subject to surveillance constituted a legally cognizable injury. However, on February 26, 2013, in *Clapper v. Amnesty International*, the U.S. Supreme Court held that the plaintiffs had not suffered a sufficiently concrete injury to have legal standing to challenge Title VII.[20] Because the Court had no jurisdiction to proceed to the merits of the plaintiffs' claims, it did not decide the merits of the plaintiffs' constitutional claim.

FISC Opinions

In August 2013, the Obama Administration partially declassified several opinions of the FISC regarding collection activities under Section702.[21] The first of these opinions, dated October 3, 2011, evaluated the targeting and minimization procedures proposed by the government to deal with new information regarding the scope of "upstream collection," in which communications are acquired from Internet traffic that is in transit from one unspecified location to another.[22] Specifically, the government had recently discovered that its upstream collection activities had acquired unrelated international communications as well as wholly domestic communications due to technological limitations.

After being presented with this new information, the FISC found the proposed minimization procedures to be deficient on statutory[23] and constitutional[24] grounds. With respect to the statutory requirements, the FISC noted that the government's proposed minimization procedures were focused "almost exclusively" on information that an analyst wished to use and not on the larger set of information that had been acquired. Consequently, communications that were known to be unrelated to a target, including those that were potentially wholly domestic, could be retained for up to five years so long as the government was not seeking to use that information. The court found that this had the effect of maximizing the retention of such information and was not consistent with FISA's mandate to minimize the retention of U.S. persons' information.[25]

The FISC also held that the proposed minimization procedures did not satisfy the Fourth Amendment.[26] The FISC found that, under the facts before it, the balance required under the Fourth Amendment's reasonableness test did not favor the government, particularly in light of the statutory deficiencies.[27]

Following the FISC's determination that the Fourth Amendment had been violated, the government presented revised minimization procedures to the FISC, and the court approved those procedures on November 30, 2011.[28] The revised minimization procedures addressed the court's

[20] Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013). *See also* CRS Report R43107, *Foreign Surveillance and the Future of Standing to Sue Post-Clapper*, by (name redacted)

[21] *See* Office of the DNI, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, August 21, 2013, available at http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

[22] Foreign Intelligence Surveillance Court Memorandum Opinion, at 29, n.24 (October 3, 2011) available at http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

[23] *Id.* at 59-63, 67-80.

[24] *Id.* at 67-79. The FISC upheld the targeting provisions, even though the government acknowledged that its upstream collection activities were known to acquire some wholly domestic communications. The FISC found that this was not a violation of Section 702, since the government could not determine "at the time of acquisition" whether a particular communication was wholly domestic. *Id.* at 46-47.

[25] *Id.* at 59.

[26] *Id.* at 67-79.

[27] *Id.* at 68, 75-78.

[28] Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (November 30, 2011) available at (continued...)

concerns by requiring the segregation of those communications most likely to involve unrelated or wholly domestic communications; requiring special handling and markings for those communications which could not be segregated; and reducing the retention period of upstream collection from five years to two.[29] With these modifications, the court found that the balancing test required under the Fourth Amendment supported the conclusion that the search was constitutionally permissible.[30]

Criminal Cases

While the *Clapper* Court dismissed the case on standing grounds, the Supreme Court did so in part relying on the fact that a criminal defendant could potentially have standing to challenge Section 702.[31] At least five criminal defendants have been notified by the government that incriminating evidence was gathered pursuant to Section 702.[32] Several of these defendants have moved to suppress such evidence, arguing that it was gathered unconstitutionally. The defendants in these cases raise Fourth Amendment[33] challenges as well as alleging that Section 702 violates Article III of the Constitution, which limits the jurisdiction of federal courts to "cases" or "controversies."[34] None of the courts to address these claims has ruled in favor of the defendants. Two cases involving criminal defendants are currently pending before the U.S. Courts of Appeals

(...continued)

http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

[29] *Id.* at 7-11.

[30] *Id.* at 14-15. A third declassified order from September 2012 addressed the question of what to do with the information that had been acquired through upstream collection prior to the October 2011 opinion. In this third opinion, the FISC acknowledged that the NSA had made a "corporate decision" to purge all data identified as originating from upstream collection before October 31, 2011 (the date that the revised minimization procedures went into effect). Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (September 2012).

[31] 50 U.S.C. §§ 1806(c), 1881e(a) (requiring notice to criminal defendants if evidence was acquired under Section 702).

[32] United States v. Hasbajrami, No. 1:11-cr-00623 (E.D.N.Y. Feb. 24, 2014); United States v. Mihalik, No. 2:11-cr-00833 (C.D. Cal. Apr. 4, 2014); United States v. Khan, No. 3:12-cr-00659 (D. Or. Apr. 3, 2014); United States v. Mohamud, No. 3:10-cr-00475 (D. Or. Nov. 19, 2013); and United States v. Muhtorov, No. 1:12-cr-00033 (D. Colo. Oct. 25, 2013).

[33] With respect to the Fourth Amendment, the defendants primarily argued that Section 702 was constitutionally defective because of the lack of a traditional warrant supported by an individualized finding of probable cause. At least three district courts have rejected the defendants' claims, reasoning that surveillance targeting foreigners who are not within the United States does not require a warrant, even if that surveillance may incidentally collect U.S. persons' communications. United States v. Muhtorov, No. 1:12-cr-00033 (D. Colo. Nov. 19, 2015) (order denying motion to suppress); United States v. Hasbajrami, No: 1:11-cr-00623 (E.D.N.Y. Mar. 8, 2016) (order denying motion to suppress); United States v. Mohamud, No. 3:10-cr-00475, 2014 WL 2866749 (D. Or. June 24, 2014) (denying motion for new trial). Furthermore, in light of the limitations and minimization procedures embodied in Section 702, those courts also concluded that the surveillance satisfied the Fourth Amendment's requirement that all searches be reasonable. *Id.*

[34] 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.... "). The claims based on Article III of the Constitution have generally argued that Section 702 does not require the FISC to evaluate the government's request in the context of "concrete facts" about a specific person or facility. While the district courts to have addressed this issue have not found in favor of the defendants, their analysis has not been uniform. *Compare* U.S. v. Mohamud, No. 3:10-cr-00475, 2014 WL 2866749 (D. Or. June 24, 2014) (finding that Section 702 mechanism did not provide advisory opinions) *with* United States v. Muhtorov, No. 1:12-cr-00033 (D. Colo. Nov. 19, 2015) (noting that Section 702 process is "qualitatively" different from traditional surveillance, but leaving question of constitutionality to "a higher court"). *See also* CRS Report R43459, *Overview of Constitutional Challenges to NSA Collection Activities*, by (name redacted), (name redacted), and (name redacted) .

for the Second and Ninth Circuits,[35] while a third is proceeding to trial in the U.S. District Court for the District of Colorado.[36]

Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov..

[35] United States v. Hasbajrami, No. 15-2684 (2nd Cir. Feb. 25, 2016) (order directing appellant to submit a proposed briefing schedule) and United States v. Mohamud, No. 14-30217 (9th Cir. Mar. 23, 2016) (noting that case is being considered for July 2016 oral argument calendar).

[36] United States v. Muhtorov, No. 1:12-cr-00033 (D. Colo. Mar. 24, 2016) (ordering parties to propose scheduling order by June 1, 2016).