Congressional Research Service
Informing the legislative debate since 1914

Origins and Impact of the Foreign Intelligence Surveillance Act (FISA) Provisions That Expired on March 15, 2020

Updated March 31, 2021

Congressional Research Service
https://crsreports.congress.gov
R40138

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R40138

March 31, 2021

Edward C. Liu
Legislative Attorney

Origins and Impact of the Foreign Intelligence Surveillance Act (FISA) Provisions That Expired on March 15, 2020

Congress enacted two amendments to the Foreign Intelligence Surveillance Act (FISA) in 2001 as part of the USA PATRIOT Act. Section 206 of the USA PATRIOT Act amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified. Section 215 enlarged the scope of materials that could be sought under FISA to include "any tangible thing." It also lowered the standard required for a court to compel their production.

Congress enacted a third FISA amendment in 2004, as part of the Intelligence Reform and Terrorism Prevention Act (IRTPA). Section 6001(a) of the IRTPA changed the rules regarding the types of individuals who may be targets of FISA-authorized searches. Also known as the "lone wolf" provision, it permits surveillance of non-U.S. persons engaged in international terrorism without requiring evidence linking those people to an identifiable foreign power or terrorist organization.

In summer 2013, media began reporting on several foreign intelligence activities conducted by the National Security Agency (NSA), including the bulk collection of telephone metadata under Section 215 of the USA PATRIOT Act. After a one-day lapse in the expiring authorities, Congress enacted the USA FREEDOM Act, which placed new limitations on the scope of the government's foreign intelligence activities, while simultaneously extending the expired provisions through March 15, 2020.

Although these provisions expired on March 15, 2020, grandfather clauses permit them to remain effective with respect to investigations that began, or potential offenses that took place, before the sunset date.

Contents

Contacts

Overview

The Foreign Intelligence Surveillance Act of 1978 (FISA) provides a statutory framework by which government agencies may, when gathering foreign intelligence for an investigation,[1] obtain authorization to conduct electronic surveillance[2] or physical searches,[3] use pen registers and trap and trace devices,[4] or access specified business records and other tangible things.[5] Authorization for such activities is typically obtained through a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created to hear the government's requests to use FISA authorities.

Shortly after the 9/11 terrorist attacks, Congress enacted the USA PATRIOT Act, in part, to "provid[e] enhanced investigative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities."[6] The Patriot Act and subsequent measures[7] amended FISA to enable the government to obtain information in a wider range of circumstances. At the time of enactment, these expanded authorities prompted concerns regarding the appropriate balance between national security interests and civil liberties. Perhaps in response to such concerns, Congress established sunset provisions that apply to three of the most controversial amendments to FISA:

- Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA), also known as the "lone wolf" provision, which simplifies the evidentiary showing needed to obtain a FISA court order to target non-U.S. persons who engage in international terrorism or activities in preparation therefor, specifically by authorizing such orders without demonstrating a link between a targeted individual and a foreign power;[8]
- Section 206 of the USA PATRIOT Act, which permits multipoint, or "roving," wiretaps (i.e., wiretaps which may follow a target even when he or she changes phones) by adding flexibility to how the subject of a FISA court order is specified;[9] and
- Section 215 of the USA PATRIOT Act, which authorizes orders compelling a person to produce "any tangible thing" that is "relevant" to an authorized foreign intelligence, international terrorism, or counter-espionage investigation.[10]

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

[2] 50 U.S.C. §§ 1801-1808.

[3] 50 U.S.C. §§ 1822-1826.

[4] 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 phone line. *See* 18 U.S.C. § 3127(3)-(4).

[5] 50 U.S.C. §§ 1861-1862.

[6] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, P.L. 107-56 (2001); H.Rept. 107-236, pt. 1, at 41 (2001).

[7] *See, e.g.*, Intelligence Reform and Terrorism Prevention Act, P.L. 108-458 (2004).

[8] *Id.* at § 6001(a), *codified* at 50 U.S.C. § 1801(b)(1)(C).

[9] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B).

[10] *Id. at* § 215, *codified at* 50 U.S.C. §§ 1861-2. Records are presumptively relevant if they pertain to a foreign power or an agent of a foreign power; the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. Additionally, if the records sought are "library circulation records, library

Congress originally set these provisions to expire on December 31, 2005, but extended the expiration dates multiple times through June 1, 2015.[11] In summer 2013, media began reporting on several foreign intelligence activities conducted by the National Security Agency (NSA), including the bulk collection of telephone metadata under Section 215. The controversy surrounding Section 215 complicated efforts to reauthorize all three of the expiring provisions, and they eventually expired on June 1, 2015. One day later, Congress enacted the USA FREEDOM Act, which placed new limitations on the scope of the government's foreign intelligence activities, while simultaneously extending the expired provisions through December 15, 2019.[12] In December 2019, Congress extended the three provisions, as amended by the USA FREEDOM Act, until March 15, 2020.[13] The provisions have not been reauthorized since they expired on March 15, 2020.

Background

The Fourth Amendment

The Fourth Amendment provides a right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[14] Many of the government activities discussed in this report could constitute a search as that term is defined in Fourth Amendment jurisprudence. Namely, government action constitutes a search when it intrudes upon a person's "reasonable expectation of privacy," which requires both that an "individual manifested a subjective expectation of privacy in the searched object" and that "society is willing to recognize that expectation as reasonable."[15]

The Fourth Amendment ultimately limits the government's ability to conduct a range of activities, such as physical searches of homes or offices, listening to phone conversations, and electronic surveillance. The Fourth Amendment requires the government to show "probable cause" and obtain a warrant issued by a "neutral and detached magistrate"[16] before conducting a search.[17] The Supreme Court has, however, recognized several exceptions to the warrant requirement.[18]

patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application must be approved by one of three high-ranking FBI officers, and cannot be further delegated.

[11] *See, e.g.*, P.L. 109-160 (extension until February 3, 2006); USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177 (extension until December 31, 2009); Department of Defense Appropriations Act, 2010, P.L. 111-118, § 1004 (2009) (extension until February 28, 2010); P.L. 111-141 (extension until February 28, 2011); P.L. 112-3 (extension until May 27, 2011); and P.L. 112-14 (extension until June 1, 2015).

[12] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, P.L. 114-23.

[13] P.L. 116-69, § 1703.

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

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

[16] Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).

[17] *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001) (recognizing a warrant exception for arrest of an individual who commits a crime in an officer's presence, as long as the arrest is supported by probable cause). Probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts." Illinois v. Gates, 462 U.S. 213, 232 (1983). For example, to issue a search warrant, probable cause requires a magistrate to determine, based on specific evidence, whether there is a "fair probability" that, for example, an area contains contraband. *Id.* at 238.

[18] *See* Riley v. California, 573 U.S. 373, 382 (2014) ("In the absence of a warrant, a search is reasonable only if it falls

These exceptions include exigent circumstances,[19] searches incident to arrest,[20] and searches with the suspect's consent.[21]

The extent to which the Fourth Amendment warrant requirement applies to the government's collection of information for intelligence gathering and other purposes unrelated to criminal investigations is unclear. Although the Supreme Court held that surveillance of wire or oral communications for criminal law enforcement purposes is subject to the Fourth Amendment's warrant requirement in 1967,[22] neither the Supreme Court nor Congress sought to regulate use of such surveillance for national security purposes at that time.

Several years later, the Supreme Court invalidated warrantless electronic surveillance of domestic organizations for national security purposes, but indicated that its conclusion might differ if the electronic surveillance targeted foreign powers or their agents.[23] A lower court has since upheld the statutory scheme governing gathering foreign intelligence information against a Fourth Amendment challenge, despite assuming that orders issued under the statute might not constitute "warrants" for Fourth Amendment purposes.[24] The Supreme Court has not yet directly addressed the issue. However, even if the Court were to hold that the warrant requirement does not apply to searches for foreign intelligence or national security purposes, such searches would presumably be subject to the general Fourth Amendment "reasonableness" test.[25]

In contrast with its surveillance rulings, the Supreme Court has not historically applied Fourth Amendment protections to documents held by third parties. In 1976, it held that the government could obtain financial records in the possession of third parties without a warrant.[26] Later, the Supreme Court likewise held that installing and using a pen register—a device used to capture telephone numbers dialed—does not constitute a Fourth Amendment search.[27] The Court reasoned that individuals have a lesser expectation of privacy for information held by third

within a specific exception to the warrant requirement.").

[19] *See, e.g.*, Illinois v. McArthur, 531 U.S. 326, 331 (2001) (stating that a warrantless seizure was not unreasonable because "it involves a plausible claim of specially pressing or urgent law enforcement need, *i.e.*, 'exigent circumstances.'").

[20] *See* Chimel v. California, 395 U.S. 752 (1969).

[21] *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

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

[23] United States v. U.S. District Court, 407 U.S. 297, 313-14, 321-24 (1972) (also called the *Keith* case, so named for the District Court judge who initially ordered disclosure of unlawful warrantless electronic surveillance to the defendants). *See also* In re Directives, 551 F.3d 1004, 1011 (Foreign Intell. Surveillance Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside the U.S. qualifies for the "special needs" exception to the warrant requirement).

[24] In re Sealed Case, 310 F.3d 717, 738-46 (Foreign Intell. Surveillance Ct. Rev. 2002).

[25] The "general reasonableness," or "totality-of-the circumstances," test 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). *See* DAVID S. KRIS & DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 11:2 (2019) ("Whether or not FISA orders are 'Warrants,' they are constitutional only if they are 'reasonable' under the Fourth Amendment.").

[26] United States v. Miller, 425 U.S. 435 (1976).

[27] Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

parties. This reasoning has been applied to noncontent data, such as the to/from address line in an email,[28] but not to communication contents—for example, the body of an email.[29]

In 2018, however, the Supreme Court held that obtaining seven days of historical cell-site location information (CSLI) from cellular telephone providers constituted a Fourth Amendment search.[30] In extending Fourth Amendment protections to CSLI, the Court reasoned that, given the ubiquity of cell phones and the fact that cell phone users can transmit CSLI simply by possessing their phones, "[o]nly the few without cell phones could escape this tireless and absolute surveillance" by law enforcement.[31] Describing its decision as "narrow," the Supreme Court declined to consider collection techniques involving foreign affairs or national security.[32]

"Title III," the Pen/Trap Statute, and FISA

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[33] and the Pen Registers and Trap and Trace Devices chapter of Title 18 ("Pen/Trap statute")[34] regulate the government's ability to conduct real-time electronic surveillance.[35] Subject to certain statutory exemptions, Title III requires the government to obtain a court order before intercepting, using, or disclosing the contents of electronic communications.[36] The Pen/Trap statute requires the government to obtain a court order before collecting noncontent information, such as phone numbers or internet headers.[37]

Enacted in 1978, FISA provides a statutory framework governing governmental authority to conduct electronic surveillance and other activities, which Fourth Amendment warrant requirements cover in domestic criminal investigations, in foreign intelligence investigations.[38] FISA's statutory requirements arguably provide a minimum standard that the government must meet before it may conduct foreign intelligence searches or surveillance.

Expiring FISA Amendments

The three amendments to FISA covered by this report are the "lone wolf," "roving wiretap," and Section 215 provisions. Although the amendments are often discussed together and may implicate

[28] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

[29] United States v. Warshak, 631 F.3d 266 (10th Cir. 2010).

[30] Carpenter v. United States,—U.S.—, 138 S. Ct. 2206, 2217 (2018).

[31] *Id.* at 2218.

[32] *Id.* at 2217, n.3.

[33] 18 U.S.C. §§ 2510-2522.

[34] 18 U.S.C. §§ 3121-3127.

[35] *See* Off. of Legal Educ. & Exec. Off. for U.S. Att'ys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009), p. 151, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[36] 18 U.S.C. § 2518.

[37] 18 U.S.C. § 3122. *See* Off. of Legal Educ. & Exec., *supra* note 37, at 152 (discussing the definition of non-content information).

[38] The scope of the Fourth Amendment warrant requirement informs the scope of activities FISA governs insofar as FISA refers to the warrant requirement in its definitions. *See* 50 U.S.C. § 1801 (restricting the definition of electronic surveillance to instances "in which a person has a reasonable expectation of privacy and *a warrant would be required for law enforcement purposes*") (emphasis added).

similar questions about the legal standards that govern the FISC's determinations, unique historical and legal issues apply to each amendment.

Access to Business Records Under Section 215

As a result of the 2013 leaks by Edward Snowden about the government's bulk collection of telephone metadata, Section 215 has become FISA's most controversial provision in recent years, as well as the provision with the greatest legislative and litigation history. Section 215 of the USA PATRIOT Act broadened federal officials' access to materials in investigations to obtain foreign intelligence information about non-United States persons or to protect against international terrorism or clandestine intelligence activities.[39] It both enlarged the scope of materials that the government may seek and lowered the standard for a court to order their production.[40]

Expansion of the Scope of Documents Subject to FISA

Before the enactment of the USA PATRIOT Act, FISA authorized the production of only four types of business records in foreign intelligence or international terrorism investigations. These were records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[41] The USA PATRIOT Act expanded the scope of records to authorize the production of "any tangible things."[42] The USA FREEDOM Act does not change the scope of documents potentially covered by Section 215.

Changes to the Standard of Review

Section 215 of the USA PATRIOT Act also modified the evidentiary standard the FISC would apply before issuing an order compelling the production of documents. Before enactment of Section 215, an applicant had to have "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[43] In contrast, under Section 215 as originally enacted, the applicant only needed to "specify that the records concerned [were] sought for a [foreign intelligence, international terrorism, or espionage investigation.]"[44] In 2005, Congress further amended FISA to change the procedures for obtaining business records. The amended procedures require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign

[39] A technical amendment to § 215 passed a few months after § 215's enactment authorizes the gathering of intelligence information that does not concern a U.S. person. *See* P.L. 107-56, § 215, *amended by* P.L. 107-108, § 314, *codified at* 50 U.S.C. § 1861.

[40] 50 U.S.C. § 1861.

[41] 50 U.S.C. § 1862(a).

[42] 50 U.S.C. § 1861(a)(1). This expanded scope drew such strong opposition from the library community that § 215 came to be known as the "library provision," despite the fact that the original text of the provision did not mention libraries. *E.g.* Richard B. Schmitt, *House Weakens Patriot Act's 'Library Provision'*, L.A. TIMES, June 16, 2005, at A-1. In response to these concerns, the USA PATRIOT Improvement and Reauthorization Act of 2005 made a library-specific amendment to the § 215 procedures. Under this amendment, one of three high-ranking FBI officers must approve the application if the records sought are "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person." Only the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security can apply for these records. This authority cannot be further delegated. 50 U.S.C. § 1861(a)(3).

[43] 50 U.S.C. § 1862(b)(2)(B).

[44] P.L. 107-56, § 215.

intelligence, international terrorism, or espionage investigation.]"[45] Under this standard, records are presumptively relevant if they pertain to

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[46]

Following the public disclosure of these bulk intelligence activities, Congress amended Section 215 in the USA FREEDOM Act to require the use of a "specific selection term" (SST) to "limit collection to the greatest extent reasonably practicable."[47] Congress defined an SST as "a term that specifically identifies a person, account, address, or personal device, or any other specific identifier." These amendments also prohibited orders under Section 215 that are limited only by broad geographic terms (such as a state or zip code) or named communications service providers (such as Verizon or AT&T).[48]

Nondisclosure and Judicial Review

Orders issued under Section 215, as amended, include nondisclosure orders prohibiting recipients from disclosing that the FBI has sought or obtained any tangible things pursuant to a FISA order. However, the recipient may discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons as permitted by the FBI.[49] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except the recipient does not have to identify attorneys with whom he has consulted.[50]

The USA PATRIOT Improvement and Reauthorization Act of 2005 provided procedures by which a Section 215 order recipient may challenge such order to produce business records.[51] Once a recipient submits a petition for review, a FISC judge must determine whether the petition is frivolous within 72 hours.[52] If the petition is frivolous, it must be denied and the order affirmed.[53] The judge may modify or set aside the order if it does not meet FISA requirements or is otherwise unlawful.[54] Either party may appeal the FISC judgment to the Foreign Intelligence Court of Review and the Supreme Court.[55]

[45] USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b).

[46] 50 U.S.C. § 1861(b)(2)(A).

[47] P.L. 114-23, § 103.

[48] *Id.* § 107.

[49] 50 U.S.C. § 1861(d)(1).

[50] 50 U.S.C. § 1861(d)(2)(C).

[51] 50 U.S.C. § 1861(f)(2)(A)(i). The Act also amended authorities related to issuing and reviewing national security letters (NSLs), among other authorities. *See, e.g.*, 18 U.S.C. § 2709.

[52] 50 U.S.C. § 1861(f)(2)(A)(ii).

[53] *Id.*

[54] 50 U.S.C. § 1861(f)(2)(B).

[55] 50 U.S.C. § 1861(f)(3).

Judicial review of nondisclosure orders operates similarly,[56] but such orders are not reviewable for one year after they are initially issued.[57] If the FISC does not find the petition to be frivolous, a nondisclosure order may be set aside if there is

> no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.[58]

The government may defeat a petition to set aside a nondisclosure order if it certifies that disclosure would endanger national security or interfere with diplomatic relations.[59] Absent a finding of bad faith, the FISC is to treat such a certification as conclusive. If a petition is denied, either due to a certification described above, frivolity, or otherwise, the petitioner may not challenge the nondisclosure order for another year.[60] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[61]

USA FREEDOM Act Call Detail Records Authority

Beginning in 2006, the government began to use FISC orders issued pursuant to Section 215 to collect domestic telephone metadata in bulk in order to help detect and identify individuals who were part of terrorist networks.[62] This program is frequently described as collecting telephone metadata "in bulk" to distinguish it from the narrower collection of metadata related to an identified individual or group of individuals that is commonplace in both law enforcement and national security investigations.

The USA FREEDOM Act amended Section 215 to establish a slightly relaxed standard to obtain such telephone metadata on an ongoing basis, but only for international terrorism investigations.[63] Whereas a standard Section 215 order would produce only records that are responsive to an approved SST, an order seeking telephone records for an international terrorism investigation can also be used to produce a second set of telephone records that *are not* responsive to an approved SST, but *are* connected to a record that an SST directly produced.[64] For example, if Alice called Bob, and Bob also called Charles, then a single Section 215 order that used Alice's phone number as an SST could obtain records of the call to Bob as well as records of Bob's call to Charles. In order to take advantage of this increased scope of production, the government would need to demonstrate to the FISC that there was a "reasonable articulable suspicion" that the SST is

[56] P.L. 109-178, § 3, added the provisions for judicial review of nondisclosure orders.

[57] 50 U.S.C. § 1861(f)(2)(A)(i).

[58] 50 U.S.C. § 1861(f)(2)(C)(i).

[59] The Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation must make these certifications. 50 U.S.C. § 1861(f)(2)(C)(ii).

[60] 50 U.S.C. § 1861(f)(2)(C)(iii).

[61] 50 U.S.C. § 1861(f)(3).

[62] Unclassified Declaration of Frances J. Fleisch, National Security Agency, Schubert v. Obama, No. 07-cv-0693-JSW at ¶ 32 (N.D. Cal. December 20, 2013) available at http://icontherecord.tumblr.com. Metadata in this context includes dialed and incoming call logs, along with the date, time, and duration of the calls. The collection of bulk metadata began at the NSA shortly after the terrorist attacks of September 11, 2001. This earlier collection did not use Section 215 authority. In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01, at 11 n.7 (FISA Ct. March 20, 2014).

[63] 50 U.S.C. § 1861(b)(2)(C). Orders issued under this authority would last for 180 days. 50 U.S.C. § 1861(c)(2)(F)(i).

[64] 50 U.S.C. § 1861(c)(2)(F)(iv).

associated with a foreign power, or an agent of a foreign power, who was engaged in international terrorism.[65]

Since Section 215's amendment, reports have surfaced describing compliance issues with the NSA's Section 215 program. On June 28, 2018, for example, the NSA publicly announced that analysts had discovered technical irregularities in some data received from telecommunications service providers, which resulted in unauthorized CDR production and required deleting three years' worth of CDRs.[66] In March 2019, the *New York Times* and *Wall Street Journal* also reported that the NSA was weighing whether to end its CDR program entirely.[67]

Despite speculation among commentators that changes in communication technologies since 2001 had lessened the utility of Section 215 collections,[68] the House passed H.R. 6172 on March 11, 2020, which would have reauthorized the provision, though not without some changes.[69] Specifically, the proposed reauthorization included amendments (1) terminating the CDR authority, and (2) prohibiting using Section 215 to acquire cellular and GPS location information or "any tangible thing" in which a person would have a reasonable expectation of privacy and a warrant would typically be required.[70] The Senate passed an amended version of H.R. 6172 on May 14, 2020. The House requested a conference on June 1, 2020, but no further action was taken.

"Lone Wolf" Terrorists

Commonly referred to as the "lone wolf" provision, Section 6001(a) of IRTPA simplifies the evidentiary standard used to determine whether an individual, other than a citizen or a permanent resident of the United States, who engages in international terrorism, may be the target of a FISA court order. It does not modify other standards used to determine the secondary question of whether the electronic surveillance or a physical search of the subject of a court order is justified in a specific situation.

Historical Context

The historical impetus for the "lone wolf" provision involved Zacarias Moussaoui, one of the individuals believed to be responsible for the 9/11 terrorist attacks. During the examination of the events leading up to the attacks, it was reported that limitations in FISA authorities hampered investigations regarding Moussaoui's involvement.[71] Specifically, FBI agents investigating Moussaoui suspected that he had planned a terrorist attack involving piloting commercial airliners, and had detained him in August 2001 on an immigration charge.[72] The FBI agents then

[65] 50 U.S.C. § 1861(b)(2)(C)(ii).

[66] *See* Nat'l Sec. Agency, NSA Reports Data Deletion (2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/ (last visited May 18, 2020).

[67] *See* Susan Landau, *Is Section 215 No Longer Worth the Effort?*, LAWFARE (Mar. 11, 2019), https://www.lawfareblog.com/section-215-no-longer-worth-effort.

[68] *Id.*

[69] H.R. 6172.

[70] *Id.*

[71] NAT'L COMM. ON TERRORIST ATTACKS UPON THE U.S., *The 9/11 Commission Report*, at 273-274 [hereinafter "*9/11 Comm'n Rep.*"]

[72] *Id.* at 273. Moussaoui, a French national, was present in the United States with an expired visa.

sought a court order under FISA to examine the contents of Moussaoui's laptop computer.[73] However, the agency apparently concluded that it had insufficient information at that time to demonstrate that Moussaoui was an agent of a foreign power as then required by FISA.[74]

Prior to its amendment, FISA authorized the FISC to approve, among other things, physical searches of a laptop only if probable cause existed to believe the laptop was owned or used by a foreign power or its agent.[75] The definition of a "foreign power" included "groups engaged in international terrorism or activities in preparation therefor."[76] Individuals involved in international terrorism for or on behalf of those groups were considered "agents of a foreign power."[77] In the weeks leading up to the attacks, it appears that the FBI encountered an actual or perceived insufficiency of information demonstrating probable cause to believe that Moussaoui was acting for or on behalf of an identifiable group engaged in international terrorism.[78]

Legislative Responses

Following these revelations, Members of Congress proposed amending the definition of "agents of a foreign power" under FISA so that individuals engaged in international terrorism need not be linked to a specific foreign power.[79] Congress enacted one such amendment by passing the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[80] Section 6001 of the legislation, known as the "lone wolf" provision, provides that persons, other than citizens or permanent residents of the United States, who are engaged in international terrorism are presumptively considered to be agents of a foreign power.[81] The provision obviates any need to provide an evidentiary connection between an individual and a foreign government or terrorist group.

Critics of the "lone wolf" provision argued that the laptop in the Moussaoui case could have been lawfully searched under FISA or the laws governing generic criminal warrants.[82] Critics also expressed concern that the simplified "lone wolf" standard would lead to "FISA serving as a substitute for some of our most important criminal laws."[83]

---

[73] *Id.* at 273-274.

[74] *Id.* at 274. Based upon this conclusion, the FBI "declined to submit a FISA application" to the FISC.

[75] 50 U.S.C. § 1821-1824.

[76] 50 U.S.C. § 1801(a)(4). At the time, foreign powers also included foreign governments, entities controlled by those governments, and factions of foreign nations and foreign-based political organizations that are not substantially composed of United States persons. *Id.* at § (a)(1-6)

[77] 50 U.S.C. § 1801(b)(2)(C).

[78] *See 9/11 Comm'n Rep.* at 274. It is unclear whether a search of Moussaoui's laptop before September 11, 2001, would have provided enough information to prevent or minimize those attacks.

[79] S. 2586, 107th Cong. (2002); S. 113, 108th Cong. (2003).

[80] S. 2845, 108th Cong. (2004) (enacted).

[81] P.L. 108-458, § 6001(a), *codified at* 50 U.S.C. § 1801(b)(1)(C). FISA also defines "agent of a foreign power" to include any person other than a United States person who "engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor." § 1801(b)(1)(D). As commentators note, § 1801(b)(1)(C) and § 1801(b)(1)(D) are similar in that neither imposes the requirement of a connection to a foreign power. David S. Kris & J. Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 8:15 (2019). However, § 1801(b)(1)(D) is not subject to sunset.

[82] *See* S.Rept. 108-40 at 33-41 (additional views of Sens. Leahy and Feingold on a similar "lone wolf" provision in S. 113).

[83] *Id.* at 73 (additional views of Sen. Feingold).

Proponents of the provision noted that the increased self-organization among terror networks has made proving connections to identifiable groups more difficult. Thus, a "lone wolf" provision is necessary to combat terrorists who use a modern organizational structure or are self-radicalized.[84]

Roving Wiretaps

Section 206 of the USA PATRIOT Act amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified.[85] It is often colloquially described as allowing FISA wiretaps to target persons rather than places.

Background

Prior to enactment of Section 206, the scope of electronic surveillance authorized by a court order was limited in two ways. First, the location or facility that was the subject of surveillance had to be identified.[86] Second, only identifiable third parties could be directed by the government to facilitate electronic surveillance.[87] Conducting electronic surveillance frequently requires the assistance of telecommunications providers, landlords, or other third parties. Furthermore, telecommunications providers are generally prohibited from assisting in electronic surveillance for foreign intelligence purposes, except as authorized by FISA.[88] In cases where the location or facility was unknown, the identity of the person needed to assist the government could not be specified in the order. Therefore, limiting the class of persons that could be directed to assist the government by a FISA court order effectively limited the reach to known and identifiable locations.

Section 206 and "Other Persons"

Section 206 of the USA PATRIOT Act amended Section 105(c)(2)(B) of FISA. It authorizes FISA orders to direct "other persons" to assist with electronic surveillance if "the Court finds, based on specific facts provided in the application, that the actions of the target ... may have the effect of thwarting the identification of a specified person."[89] In a technical amendment later that year, the requirement that the order specify the location of the surveillance was also changed so that this requirement only applies if the facilities or places are known.[90] These modifications have the effect of permitting FISA orders to direct *unspecified* individuals to assist the government in performing electronic surveillance, thus permitting court orders to authorize surveillance of places or locations that are unknown at the time the order is issued.

Congress further amended this section in the USA PATRIOT Improvement and Reauthorization Act of 2005 to require that the FISC be notified within 10 days after "surveillance begins to be

[84] S.Rept. 108-40 at 4-6. *But see* Letter from the U.S. Department of Justice to Hon. Patrick J. Leahy, at 5 (Sept. 14, 2009) (acknowledging that the amendment has not yet been relied upon in an investigation).

[85] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B).

[86] *See* 50 U.S.C. § 1805(c)(1)(B) (2001) (requiring FISA warrants to specify the "nature and location of each of the facilities or places at which electronic surveillance will be directed").

[87] *See* 50 U.S.C. § 1805(c)(2)(B) (2001).

[88] *See* 50 U.S.C. §§ 1809(a) and 1810.

[89] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B).

[90] P.L. 107-108, § 314(a)(2)(A).

directed at any new facility or place."[91] In addition, the FISC must be told the nature and location of each new facility or place, the facts and circumstances relied upon to justify the new surveillance, a statement of any proposed minimization procedures (i.e., rules to limit the government's acquisition and dissemination of information involving United States citizens) that differ from those contained in the original application or order, and the total number of facilities or places subject to surveillance under the authority of the present order.[92]

Particularity Requirement of the Fourth Amendment

The Fourth Amendment imposes specific requirements to issue warrants authorizing searches of "persons, houses, papers, and effects."[93] One of the requirements, referred to as the *particularity requirement*, states that warrants shall "particularly describ[e] the place to be searched."[94] Under FISA, roving wiretaps are not required to identify the location that may be subject to surveillance. Therefore, some may argue that roving wiretaps do not comport with the particularity requirement of the Fourth Amendment. It is not clear that the Fourth Amendment would require that searches for foreign intelligence information be supported by a warrant,[95] but prior legal challenges to similar provisions of Title III of the Omnibus Crime Control and Safe Streets Act may be instructive in the event that challenges to Section 206 are brought alleging violations of the particularity requirement of the Fourth Amendment.

Similar roving wiretaps have been permitted under Title III since 1986 in cases where the target of the surveillance takes actions to thwart such surveillance.[96] The procedures under Title III are similar to those currently used under FISA, with two significant differences. First, a roving wiretap under Title III must definitively identify the target of the surveillance.[97] Fixed wiretaps under Title III and all wiretaps under FISA need only identify the target if the target's identity is known. FISA permits roving wiretaps via court orders that only provide a specific description of the target.[98] Second, Title III requires that the surveilled individuals be notified of the surveillance, generally 90 days after surveillance terminates.[99] FISA contains no similar notification provision.

In *United States v. Petti*, the U.S. Court of Appeals for the Ninth Circuit considered a challenge to a roving wiretap under Title III alleging that roving wiretaps do not satisfy the particularity requirement of the Fourth Amendment.[100] The court initially noted that

> the test for determining the sufficiency of the warrant description is whether the place to be searched is described with sufficient particularity to enable the executing officer to

[91] P.L. 109-177, § 108(b)(4), *codified at* 50 U.S.C. § 1805(c)(3). This deadline for notification can be extended to up to 60 days by the FISC upon a showing of good cause.

[92] *Id.*

[93] U.S. CONST. amend. IV. The Supreme Court has held that electronic surveillance of private conversations qualifies as a search for purposes of the Fourth Amendment. *See* Katz v. United States, 389 U.S. 347 (1967).

[94] *Id.*

[95] *See supra* footnotes 16-17 and accompanying text.

[96] Electronic Communications Privacy Act of 1986, P.L. 99-508, § 106(d)(3), *codified at* 18 U.S.C. § 2518(11).

[97] 18 U.S.C. § 2518(11)(b)(ii).

[98] *See* 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(A).

[99] 18 U.S.C. § 2518(8)(d). This notification may be postponed upon an ex parte showing of good cause.

[100] 973 F.2d 1441 (9th Cir. 1992).

> locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.[101]

Applying this test, the Ninth Circuit held that roving wiretaps under Title III satisfied the particularity clause of the Fourth Amendment.[102] The court relied upon the fact that targets of roving wiretaps have to be identified and that such wiretaps are only available where the target's actions indicate an intent to thwart electronic surveillance.[103]

Critics of roving wiretaps under FISA may argue that Section 206 increases the likelihood that innocent conversations will be the subject of electronic surveillance. They may further argue that the threat of these accidental searches of innocent persons is precisely the type of injury sought to be prevented by the particularity clause of the Fourth Amendment. Such a threat may be particularly acute in this case given the fact that there is no requirement under FISA that the target of a roving wiretap be identified, although the target must be specifically described.[104]

Effect of Sunset Provisions

As noted above, Congress extended these three FISA amendments until March 15, 2020, but they have since lapsed. Consequently, the amended FISA authorities have reverted to their text as it appeared before the enactment of the USA PATRIOT Act. For example, in the context of roving wiretaps, Section 105(c)(2) of FISA now reads as it did on October 25, 2001,[105] eliminating the authority for FISA court orders to direct other unspecified persons to assist with electronic surveillance.[106] Likewise, regarding FISA orders for the production of documents, Sections 501 and 502 of FISA read as they did on October 25, 2001,[107] restricting the types of business records that are subject to FISA and reinstating the requirement for "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[108] Moreover, Section 215's CDR authority has also lapsed given that it was not subject to a separate sunset.

However, a grandfather clause applies to each of the three provisions.[109] The grandfather clauses authorize the continued effect of the amendments with respect to investigations that began, or

[101] *Id.* at 1444 (internal quotation marks omitted).

[102] *Id.* at 1445.

[103] *Id. See also* United States v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993) (similarly holding constitutional a provision authorizing roving bugs under Title III).

[104] 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(B).

[105] P.L. 109-177, § 102(b). The relevant section of FISA will then provide

> that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance. 50 U.S.C. § 1805(c)(2) (2001).

[106] The sunset will not repeal the provision of FISA that permits a FISA warrant to omit the identity of facilities or places that will be subject to electronic surveillance. However, the authority for most new roving wiretaps may be effectively repealed because new orders may not direct unspecified persons to assist with surveillance.

[107] P.L. 109-177, § 102(b). Access will then be limited to records held by common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862(c)(2) (2001).

[108] 50 U.S.C. § 1862(b)(2)(B) (2001).

[109] None of the extensions have affected the grandfather provisions.

potential offenses that took place, before the provisions' sunset date.[110] Thus, for example, if a non-U.S. person were engaged in international terrorism before the sunset date, he would still be considered a "lone wolf" for FISA court orders sought after the provision expired. Similarly, if an individual was engaged in international terrorism before that date, he may be the target of a roving wiretap under FISA even if authority for new roving wiretaps expired.

Author Information

Edward C. Liu
Legislative Attorney

Disclaimer

[110] P.L. 107-56, § 224(b); P.L. 108-458, § 6001(b) (referencing PATRIOT Act sunset provision in P.L. 107-56, § 224(b)).