Congressional Research Service
Informing the legislative debate since 1914

Amendments to the Foreign Intelligence Surveillance Act (FISA) Expiring on December 15, 2019

Updated April 11, 2016

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

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Two amendments to the Foreign Intelligence Surveillance Act (FISA) were enacted 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 before a court order may be issued to compel their production.

A third amendment to FISA was enacted 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 persons 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 December 15, 2019.

Although these provisions are set to sunset at the end of 2019, 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 (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] utilize 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 via a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created to act as a neutral judicial decisionmaker in the context of FISA.

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] That act and subsequent measures[7] amended FISA to enable the government to obtain information in a greater number 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 which 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 in the absence of a proven 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 the manner in which 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 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) (definition of "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 considered 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,

These provisions were originally set to expire on December 31, 2005, but were extended multiple times, with slight modifications, 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]

Background

FISA, enacted in 1978, provides a statutory framework which governs governmental authority to conduct, as part of an investigation to gather foreign intelligence information, electronic surveillance and other activities to which the Fourth Amendment warrant requirement would apply if they were conducted as part of a domestic criminal investigation.[13] Its statutory requirements arguably provide a minimum standard that must be met before foreign intelligence searches or surveillance may be conducted by the government.[14]

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 as a group and may implicate similar questions regarding what legal standards 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 leaks by Edward Snowden, Section 215 has come to be the most controversial provision in recent years, as well as the provision with the most extensive legislative and

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," 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] The scope of activities governed by FISA relates to the scope of the Fourth Amendment warrant requirement insofar as the statute 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).

[14] But see CRS Report R40888, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea, at 29-33 ("While the congressional intent to cabin the President's exercise of any inherent constitutional authority to engage in foreign intelligence electronic surveillance may be clear from the exclusivity provision in FISA and from the legislative history of the measure, some support may be drawn from the [Foreign Intelligence Surveillance] Court of Review's decision in In re Sealed Case for the position that the President continues to have the power to authorize warrantless electronic surveillance to gather foreign intelligence outside the FISA framework").

litigation history. Section 215 of the USA PATRIOT Act broadened federal officials' access to materials in investigations to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[15] It both enlarged the scope of materials that may be sought and lowered the standard for a court to issue an order compelling their production.[16]

Expansion of the Scope of Documents Subject to FISA

Prior to 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.[17] The USA PATRIOT Act expanded the scope of records to authorize the production of "any tangible things."[18] The scope of documents potentially covered by Section 215 was not changed by the USA FREEDOM Act.

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. Prior to 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."[19] 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.]"[20] In 2005, Congress further amended FISA procedures for obtaining business records. The applicable standard was changed to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence, international terrorism, or espionage investigation.]"[21] 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

[15] The gathering of intelligence information not concerning a U.S. person was authorized by a technical amendment to § 215 passed a few months after its enactment. *See* P.L. 107-56, § 215, *amended by* P.L. 107-108, § 314, *codified at* 50 U.S.C. § 1861.

[16] 50 U.S.C. § 1861.

[17] 50 U.S.C. § 1862(a).

[18] 50 U.S.C. § 1861(a)(1). This expanded scope drew strong opposition from the library community, so much so 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, a library-specific amendment was made to the § 215 procedures by the USA PATRIOT Improvement and Reauthorization Act of 2005. Under this amendment, 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," the application must be approved by one of three high-ranking FBI officers. Applications for these records could be made only by 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. This authority cannot be further delegated. 50 U.S.C. § 1861(a)(3).

[19] 50 U.S.C. § 1862(b)(2)(B).

[20] P.L. 107-56, § 215.

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

- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[22]

Beginning in 2006, the government began to use orders of the FISC issued pursuant to Section 215 to collect large amounts of domestic telephone metadata in bulk with the goal of helping to detect and identify individuals who were part of terrorist networks.[23] This program is frequently described as collecting telephone metadata "in bulk" to distinguish it from the narrower collection of metadata pertaining to an identified individual or group of individuals that is commonplace in both law enforcement and national security investigations.[24]

Following the public disclosure of these bulk intelligence activities, Section 215 was amended by the USA FREEDOM Act to additionally require the use of a "specific selection term" (SST) to "limit collection to the greatest extent reasonably practicable."[25] An SST was defined as "a term that specifically identifies a person, account, address, or personal device, or any other specific identifier." These amendments also expressly 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).[26]

A slightly relaxed standard can be used under the amended Section 215 to obtain telephone metadata on an ongoing basis, but only for international terrorism investigations.[27] Whereas a standard order under Section 215 would produce only those 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* themselves responsive to an approved SST, but that *are* connected to one of the records that was directly produced by an SST.[28] 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 the call from Bob 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 associated with a foreign power, or an agent of a foreign power, who was engaged in international terrorism.[29]

[22] 50 U.S.C. § 1861(b)(2)(A).

[23] 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 had begun at the NSA shortly after the terrorist attacks of September 11, 2001. This earlier collection did not use the authority of Section 215. 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).

[24] A number of lawsuits were also filed by private citizens and advocacy groups alleging that the bulk collection under Section 215 violated both constitutional and statutory provisions. See CRS Report R43459, *Overview of Constitutional Challenges to NSA Collection Activities*, by Edward C. Liu, Andrew Nolan, and Richard M. Thompson II. These suits have largely been rendered moot by the enactment of the USA FREEDOM Act, with the exception of plaintiffs' requests to delete information previously collected.

[25] P.L. 114-23, § 103.

[26] *Id.* § 107.

[27] *Id.* § 101. Codified at 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).

[28] 50 U.S.C. § 1861(c)(2)(F)(iv).

[29] 50 U.S.C. § 1861(b)(2)(C)(ii).

Nondisclosure and Judicial Review

Orders issued under Section 215, as amended, are accompanied by nondisclosure orders prohibiting the 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.[30] The recipient must identify persons to whom disclosure has been made, or is intended to be made, if the FBI requests, except that attorneys with whom the recipient has consulted do not need to be identified.[31]

The USA PATRIOT Improvement and Reauthorization Act of 2005 provided procedures by which a recipient of a Section 215 order may challenge orders compelling the production of business records.[32] Once a petition for review is submitted by a recipient, a FISC judge must determine whether the petition is frivolous within 72 hours.[33] If the petition is frivolous, it must be denied and the order affirmed.[34] The order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[35] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[36]

Judicial review of nondisclosure orders operates under a similar procedure,[37] but such orders are not reviewable for one year after they are initially issued.[38] If the petition is not determined 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.[39]

A petition to set aside a nondisclosure order may be defeated if the government certifies that disclosure would endanger the national security or interfere with diplomatic relations.[40] Absent any finding of bad faith, such a certification is to be treated as conclusive by the FISC. 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.[41] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[42]

[30] 50 U.S.C. § 1861(d)(1).

[31] 50 U.S.C. § 1861(d)(2)(C).

[32] 50 U.S.C. § 1861(f)(2)(A)(i).

[33] 50 U.S.C. § 1861(f)(2)(A)(ii).

[34] *Id.*

[35] 50 U.S.C. § 1861(f)(2)(B).

[36] 50 U.S.C. § 1861(f)(3).

[37] Judicial review of nondisclosure orders was added by P.L. 109-178, § 3.

[38] 50 U.S.C. § 1861(f)(2)(A)(i).

[39] 50 U.S.C. § 1861(f)(2)(C)(i).

[40] Such certifications must be made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation. 50 U.S.C. § 1861(f)(2)(C)(ii).

[41] 50 U.S.C. § 1861(f)(2)(C)(iii).

[42] 50 U.S.C. § 1861(f)(3).

"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 investigations regarding Moussaoui's involvement were hampered by limitations in FISA authorities.[43] 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.[44] The FBI agents then sought a court order under FISA to examine the contents of Moussaoui's laptop computer.[45] 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.[46]

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.[47] The definition of a "foreign power" included "groups engaged in international terrorism or activities in preparation therefor."[48] Individuals involved in international terrorism for or on behalf of those groups were considered "agents of a foreign power."[49] 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.[50]

Legislative Responses

Following these revelations, a number of legislative proposals were put forth to amend 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.[51] One such amendment was ultimately

---

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

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

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

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

[47] 50 U.S.C. § 1821-1824.

[48] 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)

[49] 50 U.S.C. § 1801(b)(2)(C).

[50] *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.

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

enacted with passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[52] 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.[53] 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.[54] 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."[55]

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 who are self-radicalized.[56]

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.[57] 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.[58] Second, only identifiable third parties could be directed by the government to facilitate electronic surveillance.[59] 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.[60] 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.

---

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

[53] P.L. 108-458, § 6001(a), *codified at* 50 U.S.C. § 1801(b)(1)(3).

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

[55] *Id.* at 73 (additional views of Senator Feingold).

[56] 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).

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

[58] *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").

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

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

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."[61] 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.[62] 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.

This section was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005 to require that the FISC be notified within 10 days after "surveillance begins to be directed at any new facility or place."[63] 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.[64]

Particularity Requirement of the Fourth Amendment

The Fourth Amendment imposes specific requirements upon the issuance of warrants authorizing searches of "persons, houses, papers, and effects."[65] One of the requirements, referred to as the particularity requirement, states that warrants shall "particularly describ[e] the place to be searched."[66] 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,[67] 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.[68] The procedures under Title III are similar to those currently used under FISA, but two significant differences exist. First, a roving wiretap under Title III must definitively identify the target of the surveillance.[69] Fixed wiretaps

---

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

[62] P.L. 107-108, § 314(a)(2)(A).

[63] 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.

[64] *Id.*

[65] 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).

[66] *Id.*

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

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

[69] 18 U.S.C. § 2518(11)(b)(ii).

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.[70] Second, Title III requires that the surveilled individuals be notified of the surveillance, generally 90 days after surveillance terminates.[71] FISA contains no similar notification provision.

In *United States v. Petti*, the U.S. Court of Appeals for the Ninth Circuit was presented with a challenge to a roving wiretap under Title III alleging that roving wiretaps do not satisfy the particularity requirement of the Fourth Amendment.[72] 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 locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.[73]

Applying this test, the Ninth Circuit held that roving wiretaps under Title III satisfied the particularity clause of the Fourth Amendment.[74] The court in this case relied upon the fact that targets of roving wiretaps had to be identified and that they were only available where the target's actions indicated an intent to thwart electronic surveillance.[75]

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.[76]

Effect of Sunset Provisions

As noted above, these three FISA amendments have been extended until December 15, 2019. If that date were to arrive without any extension, the amended FISA authorities would revert 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 would read as it did on October 25, 2001,[77] eliminating the authority for FISA court orders to direct other unspecified persons to assist with electronic surveillance.[78] Likewise, regarding FISA orders for the production of documents,

---

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

[71] 18 U.S.C. § 2518(8)(d). This notification may be postponed upon an ex parte showing of good cause.

[72] 973 F.2d 1441 (9th Cir. 1992).

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

[74] *Id.* at 1445.

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

[76] 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(B).

[77] 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).

[78] The sunset will not repeal the provision of FISA that permits a FISA warrant to omit the identify of facilities or

Sections 501 and 502 of FISA would read as they did on October 25, 2001,[79] 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."[80]

However, a grandfather clause applies to each of the three provisions.[81] The grandfather clauses authorize the continued effect of the amendments with respect to investigations that began, or potential offenses that took place, before the provisions' sunset date.[82] 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 has expired. Similarly, if an individual is 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

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.

[79] 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).

[80] 50 U.S.C. § 1862(b)(2)(B) (2001).

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

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