Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire in 2009

Anna C. Henning
Legislative Attorney

Edward C. Liu
Legislative Attorney

October 29, 2009

Congressional Research Service
7-5700
www.crs.gov
R40138

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Three amendments to the Foreign Intelligence Surveillance Act (FISA) are set to expire (sunset) on December 31, 2009. S. 1692, a bill reported favorably by the Senate Judiciary Committee with an amendment in the nature of a substitute, would extend the sunset date by four years and make various modifications to existing authorities. H.R. 3845 would likewise establish a new sunset of December 31, 2013, but it would reauthorize only two of the three expiring provisions.

The three sunsetting amendments expanded the scope of federal intelligence-gathering authority following the 9/11 terrorist attacks. Two 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.

The third amendment was enacted in 2004, as part of the Intelligence Reform and Terrorism Protection 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.

Although these provisions are set to sunset on December 31, 2009, 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 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 decision maker 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.

The 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. These amendments include:

- Section 6001(a) of the Intelligence Reform and Terrorism Protection 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

[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) (2008) (definition of "foreign intelligence information").

[2] 50 U.S.C. §§ 1801-1808 (2008).

[3] 50 U.S.C. §§ 1822-1826 (2008).

[4] 50 U.S.C. §§ 1841-1846 (2008). 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) (2008).

[5] 50 U.S.C. §§ 1861-1862 (2008).

[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 Protection Act, P.L. 108-458 (2004).

[8] *Id.* at § 6001(a), *codified* at 50 U.S.C. § 1801(b)(1)(C) (2008).

[9] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

- Section 215 of the USA PATRIOT Act, which broadens the types of records and other tangible things that can be made accessible to the government under FISA.[10]

Although the amendments were initially set to expire in 2005, a 2005 reauthorization measure set a new sunset date of December 31, 2009.[11] While leaving the expansions of authority generally intact, Congress modified the three amendments as part of the 2005 reauthorization act and various other measures.[12]

The impending sunset date has prompted congressional interest and several legislative proposals regarding the expiring provisions. Most prominently, S. 1692, a bill reported favorably by the Senate Judiciary Committee with an amendment in the nature of a substitute, would extend the provisions for an additional four years. This report discusses background information, the three expiring provisions, and relevant legislative proposals.

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]

Distinction Between FISA Court Orders and Warrants in Criminal Investigations

The Fourth Amendment to the U.S. Constitution protects against "unreasonable searches and seizures."[15] In domestic criminal law investigations, it generally requires law enforcement

[10] *Id. at* § 215, *codified at* 50 U.S.C. §§ 1861-2 (2008).

[11] *See* USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177 (2006).

[12] *See, e.g.*, An act to amend the USA PATRIOT Act to extend the sunset of certain provisions of that Act and the lone wolf provision of the Intelligence Reform and Terrorism Prevention Act of 2004 to July 1, 2006, P.L. 109-160 (2005); USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178 (2006); Protect America Act of 2007, P.L. 110-55 (2007); FISA Amendments Act of 2008, P.L. 110-261 (2008).

[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 WD00002, *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").

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

officers to obtain a court-issued warrant before conducting a search.[16] When the warrant requirement does not apply, government activity is generally subject to a "reasonableness" test under the Fourth Amendment.[17]

The extent to which the warrant requirement applies to the government's collection of foreign intelligence is unclear. In a 1972 case, the Supreme Court invalidated warrantless electronic surveillance of domestic organizations on Fourth Amendment grounds, despite the government's assertion of a national security rationale.[18] However, it indicated that its conclusion might be different in a future case involving the electronic surveillance of foreign powers or their agents, within or outside the United States.[19] In a 2002 case, the Foreign Intelligence Surveillance Court of Review upheld FISA, as amended by the USA PATRIOT Act, against a Fourth Amendment challenge.[20] The court assumed, without deciding the question, that FISA court orders do not constitute warrants for purposes of the Fourth Amendment analysis. Relying on a general reasonableness analysis, it nonetheless upheld such orders, emphasizing both the privacy protections in the statutory framework and the governmental interest in preventing national security threats.[21]

Thus, although they apply to similar government activities, different standards govern FISA court orders and warrants issued by judges in criminal investigations. Search warrants in the general criminal law context must be justified by indicia of criminal conduct. In contrast, a substantial purpose of court orders obtained pursuant to FISA must be the collection of foreign intelligence information.[22] Although both FISA orders and criminal warrants require impartial judicial review to determine whether probable cause exists, the propositions that must be supported by probable cause are substantially different in the two frameworks. In the case of a FISA court order, the FISC, in authorizing electronic surveillance or a physical search, must find probable cause to believe both (1) that the person targeted by the order is a foreign power or its agent, and (2) that the subject of the search (i.e., the telecommunications or place to be searched) is owned, possessed, or will be used by the target.[23]

---

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

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

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

[19] *Id.* at 321-22. *See also* In re Directives, 2008 U.S. App. LEXIS 27417 (U.S. Foreign Intell. Surveillance Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the U.S. qualifies for the "special needs" exception to the warrant requirement); CRS Report WD00002, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea, at 9-12 (discussing courts' differing application of the Fourth Amendment to searches for the purpose of foreign intelligence collection).

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

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

[22] *See, e.g.*, 50 U.S.C. § 1804(a)(7)(B) (2008). Prior to 2001, the statute had required that "the purpose" of a FISA warrant be foreign intelligence collection.

[23] 50 U.S.C. § 1805(a)(3) (2008) (electronic surveillance); *Id.* at § 1824(a)(3) (physical searches). In contrast, federal criminal search warrants require probable cause to believe that instrumentalities, evidence, or fruits of a crime will be found in the place to be searched. *See* Fed. R. Crim. P. 41(c). Criminal warrants authorizing electronic surveillance (continued...)

Distinction Between FISA Court Orders and National Security Letters

Among the more complex questions regarding the expiring FISA amendments are those concerning authorities for the production of business records and other tangible materials. One reason for the complexity is that national security letters provide an overlapping source of authority in some circumstances. National security letters, which are analogous to administrative subpoenas and are authorized by five federal statutes,[24] require businesses to produce specified records to federal officials in national security investigations.[25] As a practical matter, national security letters are issued much more frequently than are FISA court orders for the production of documents. In 2006, for example, less than 50 such FISA orders were issued, compared with the FBI's issuance of more than 50,000 national security letters.[26] However, FISA court orders provide access to categories of records and other tangible things not available via national security letters, which are relatively limited in scope.

Like orders issued pursuant to FISA, national security letters are justified by national interests other than criminal law enforcement and are often presumed to be exempt from the Fourth Amendment warrant requirement.[27] They differ from FISA orders in several respects, however. FISA orders must be obtained from the FISC; national security letters are issued directly by federal agency officials. In addition, as mentioned, the scope of documents which may be obtained pursuant to a national security letter is more limited than that which might be authorized in a FISA order. As mentioned, the authority for national security letters is derived from five statutes, each of which pertains to only a narrow category of documents.[28]

The USA PATRIOT Act expanded authorities for the issuance of national security letters. For example, key amendments extended issuing authority to the Special Agents in Charge at FBI field offices. The authority had previously been limited to officials at FBI headquarters. It also extended issuing authority in some circumstances to officials from federal agencies other than the FBI. Other provisions addressed the government's authority to prohibit recipients of national

(...continued)

additionally require probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are insufficient, and that the facilities that are the subject of surveillance will be used by the target. 18 U.S.C. § 2518(3) (2008).

[24] *See infra* note 28 and accompanying text.

[25] For a detailed examination of national security letters, see CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle.

[26] *See* OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, Mar. 2008, http://www.usdoj.gov/oig/special/s0803b/final.pdf; OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006*, Mar. 2008, available at http://www.usdoj.gov/oig/special/s0803a/final.pdf.

[27] Support for the exemption may be found in a 1976 Supreme Court case, *U.S. v. Miller*, 425 U.S. 435 (1976), in which the Court held that the warrant requirement does not apply to an individual's bank account records.

[28] *See* 12 U.S.C. § 3414(a)(5) (records of 21 specified types of financial institutions); 18 U.S.C. § 2709 (records of telecommunications providers); 15 U.S.C. §§ 1681u, 1681v (credit reports); and 50 U.S.C. § 436 (various specified types of records related to the finances and travel of government employees, which may be obtained only in investigations involving alleged leaks of classified information by such employees).

security letters to disclose that they have received such requests. Such authorities have been modified since the USA PATRIOT Act by legislation and judicial decisions.[29]

Additional USA PATRIOT Act amendments to national security letter authorities resembled the § 215 amendment governing FISA orders for the production of documents, discussed *infra*. In both cases, the relevant amendments broadened the predicate circumstances which trigger authority for the request of documents. National security letters previously required the government to demonstrate a connection to a foreign power or its agent. The USA PATRIOT Act amendments authorize their issuance when documents sought are shown to be relevant to an investigation to protect against international terrorism or foreign spying. The § 215 amendment makes an analogous change. Unlike the § 215 amendment, however, the national security letter amendment contains no sunset provision.

Expiring FISA Amendments

As discussed, three amendments to FISA are set to sunset at the end of 2009—the "lone wolf," "roving wiretap," and § 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.

"Lone Wolf" Terrorists

Commonly referred to as the "lone wolf" provision, § 6001(a) of IRTPA simplifies the evidentiary standard used to determine whether an individual, other than a citizen or a permanent resident of the U.S., 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.[30] Specifically, FBI agents investigating Moussaoui suspected that he had planned a terrorist attack involving piloting

[29] The 2005 reauthorization of the USA PATRIOT Act, P.L. 109-177, created a judicial enforcement mechanism, tightened and clarified the circumstances in which an agency can prohibit a provider from disclosing the receipt of a national security letter, expanded congressional oversight, and called for an audit by the Justice Department Office of the Inspector General, among other measures. Judicial decisions preceding the reauthorization measure had struck down provisions which denied judicial review and prohibited disclosure. *See* Doe v. Ashcroft, 334 F.Supp.2d 471 (S.D.N.Y. 2004); Doe v. Gonzales, 386 F.Supp.2d 66 (D.Conn. 2005). In a decision which post-dates the reauthorization, *John Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), the U.S. Court of Appeals for the Second Circuit held that the national security letter provision related to electronic communications records is unconstitutional to the extent that it imposes a nondisclosure requirement without government-initiated judicial review in which the government bears the burden of proving that nondisclosure is necessary.

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

commercial airliners, and had detained him in August of 2001 on an immigration charge.[31] The FBI agents then sought a court order under FISA to examine the contents of Moussaoui's laptop computer.[32] 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.[33]

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.[34] The definition of a "foreign power" included "groups engaged in international terrorism or activities in preparation therefor."[35] Individuals involved in international terrorism for or on behalf of those groups were considered "agents of a foreign power."[36] 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.[37]

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.[38] One such amendment was ultimately enacted with passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[39] Section 6001 of the legislation, known as the "lone wolf" provision, provides that persons, other than citizens or permanent residents of the U.S., who are engaged in international terrorism are presumptively considered to be agents of a foreign power.[40] 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.[41] 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."[42]

---

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

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

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

[34] 50 U.S.C. § 1821-1824 (2001).

[35] 50 U.S.C. § 1801(a)(4) (2001). 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)

[36] 50 U.S.C. § 1801(b)(2)(C) (2001).

[37] *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.

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

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

[40] P.L. 108-458, § 6001(a), *codified at* 50 U.S.C. § 1801(b)(1)(3) (2008).

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

[42] *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 who are self-radicalized.[43]

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.[44] It is often colloquially described as allowing FISA wiretaps to target persons rather than places.

Background

Prior to enactment of § 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.[45] Second, only identifiable third parties could be directed by the government to facilitate electronic surveillance.[46] 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.[47] 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 § 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."[48] 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.[49] 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.

---

[43] 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).

[44] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

[45] *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").

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

[47] *See* 50 U.S.C. §§ 1809(a) and 1810 (2008).

[48] P.L. 107-56, § 206, *codified at* 50 U.S.C. § 1805(c)(2)(B) (2008).

[49] P.L. 107-108, § 314(a)(2)(A).

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."[50] 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.[51]

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."[52] One of the requirements, referred to as the particularity requirement, states that warrants shall "particularly describ[e] the place to be searched."[53] 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,[54] 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 § 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.[55] 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.[56] 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.[57] Second, Title III requires that the surveilled individuals be notified of the surveillance, generally 90 days after surveillance terminates.[58] 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.[59] The court initially noted that:

---

[50] P.L. 109-177, § 108(b)(4), *codified at* 50 U.S.C. § 1805(c)(3) (2008). This deadline for notification can be extended to up to 60 days by the FISC upon a showing of good cause.

[51] *Id.*

[52] 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).

[53] *Id.*

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

[55] Electronic Communications Privacy Act of 1986, P.L. 99-508, § 106(d)(3), *codified at* 18 U.S.C. § 2518(11) (2008).

[56] 18 U.S.C. § 2518(11)(b)(ii) (2008).

[57] *See* 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(A) (2008).

[58] 18 U.S.C. § 2518(8)(d) (2008). This notification may be postponed upon an ex parte showing of good cause.

[59] 973 F.2d 1441 (9th Cir. 1992).

> ... 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.[60]

Applying this test, the Ninth Circuit held that roving wiretaps under Title III satisfied the particularity clause of the Fourth Amendment.[61] 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.[62]

Critics of roving wiretaps under FISA may argue that § 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.[63]

Access to Business Records Under FISA

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.[64] 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. In all investigations, the production of items pertaining to a U.S. person may not be compelled solely upon the basis of activities protected by the First Amendment to the Constitution.[65]

Background

In 1976, the Supreme Court held that an individual's bank account records did not fall within the protection of the Fourth Amendment's prohibition on unreasonable searches and seizures.[66] Subsequently, Congress passed laws protecting various types of transactional information, but built in exceptions to provide some access to statutorily protected records sought for counter intelligence purposes.[67] These exceptions comprise the authority for national security letters,

---

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

[61] *Id.* at 1445.

[62] *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).

[63] 50 U.S.C. §§ 1804(a)(3), 1805(c)(1)(B) (2008).

[64] 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 (2008).

[65] 50 U.S.C. § 1861(a) (2008).

[66] U.S. v. Miller, 425 U.S. 435 (1976). The rationale was that persons have a diminished expectation of privacy when information sought has already been revealed to a third party.

[67] *See* CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle, at 3-4.

discussed *supra*, which are relied upon to compel the production of records in limited circumstances.

In 1998, Congress first amended FISA to authorize the production of documents not available through national security letters. Four types of documents initially could be sought in foreign intelligence or international terrorism investigations, including records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[68] Applications for orders under this section had to be made by FBI agents with a rank of Assistant Special Agent in Charge or higher and investigations could not be conducted solely on the basis of activities protected by the First Amendment.[69] Under these procedures the FISC would issue an order if, *inter alia*, the application contained "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."[70] Recipients of an order under this section were required to comply with it, and were also prohibited from disclosing to others that an order had been issued.[71]

Expansion of the Scope of Documents Subject to FISA

As mentioned, § 215 of the USA PATRIOT Act made several changes to the procedures under FISA for obtaining business records.[72] Among these was an expansion of the scope of records that are subject to compulsory production. Prior to the USA PATRIOT Act amendment, only records from the four categories of businesses mentioned above could be obtained. In contrast, § 215 authorizes the production of "any tangible things."[73]

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.[74] Opposition from this group appears to have been primarily based upon the chilling effect such access could have on the exercise of First Amendment rights and purported intrusions into areas protected by the Fourth Amendment.[75] Opposition from library advocates may have also been a residual response to prior attempts by the FBI to gather foreign intelligence information from library staff during the Cold War.[76]

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

[68] 50 U.S.C. § 1862(a) (2001).

[69] 50 U.S.C. § 1862(a)(1) (2001).

[70] 50 U.S.C. § 1862(b)(2)(B) (2001).

[71] 50 U.S.C. § 1862(d)(1)-(2) (2001).

[72] P.L. 107-56, § 215 *codified at* 50 U.S.C. § 1862(a)-(b) (2008).

[73] 50 U.S.C. § 1861(a)(1) (2008).

[74] *E.g.* Richard B. Schmitt, *House Weakens Patriot Act's 'Library Provision'*, L.A. TIMES, June 16, 2005, at A-1.

[75] *See, e.g.*, AMERICAN LIBRARY ASSOCIATION, *Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users*, Jan. 29, 2003, available at http://www.ala.org; Judith King, Director ALA Office for Intellectual Freedom, Letter to the Editor, *FBI 'Fishing Expeditions' Librarians' Biggest Worry*, WALL ST. J., May 24, 2004, at A15; David Mehegan, *Reading Over Your Shoulder: The Push Is On To Shelve Part Of The Patriot Act*, BOSTON GLOBE, Mar. 9, 2004, at E5.

[76] *See* Ulrika Ekman Ault, *The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?*, 65 N.Y.U. L. REV. 1532 (1990).

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.[77]

Changes to the Standard of Review

Section 215 of the USA PATRIOT Act also modified the standard for the FISC to issue an order compelling the production of documents. Prior to enactment of § 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."[78] In contrast, under § 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.]"[79]

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.]"[80] 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.

Nondisclosure and Judicial Review

Orders issued under § 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.[81] 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.[82]

The USA PATRIOT Improvement and Reauthorization Act of 2005 provided procedures by which a recipient of a § 215 order may challenge orders compelling the production of business records.[83] Once a petition for review is submitted by a recipient, a FISC judge must determine

[77] 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) (2008).

[78] 50 U.S.C. § 1862(b)(2)(B) (2001).

[79] P.L. 107-56, § 215.

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

[81] 50 U.S.C. § 1861(d)(1) (2008).

[82] 50 U.S.C. § 1861(d)(2)(C) (2008).

[83] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

whether the petition is frivolous within 72 hours.[84] If the petition is frivolous, it must be denied and the order affirmed.[85] The order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[86] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[87]

Judicial review of nondisclosure orders operates under a similar procedure,[88] but such orders are not reviewable for one year after they are initially issued.[89] 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.[90]

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.[91] 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.[92] Appeals by either party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[93]

DOJ OIG Report

The USA PATRIOT Improvement and Reauthorization Act of 2005 directed the Inspector General of the Department of Justice (OIG) to audit the FBI's use of § 215 authority and report its findings to Congress.[94] An unclassified version of the OIG's audit for calendar year 2006 was released in March of 2008.[95] According to the report, the number of requests for § 215 orders submitted to the FISC in 2006 totaled 47, although more than half were requests to renew or extend previous orders. The FISC granted all 47 of the requests submitted that year. However, six additional requests were processed but withdrawn before formal consideration by the FISC. The

[84] 50 U.S.C. § 1861(f)(2)(A)(ii) (2008).

[85] *Id.*

[86] 50 U.S.C. § 1861(f)(2)(B) (2008).

[87] 50 U.S.C. § 1861(f)(3) (2008).

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

[89] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).

[90] 50 U.S.C. § 1861(f)(2)(C)(i) (2008).

[91] 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) (2008).

[92] 50 U.S.C. § 1861(f)(2)(C)(iii) (2008).

[93] 50 U.S.C. § 1861(f)(3) (2008).

[94] P.L. 109-177, § 106A.

[95] OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006*, Mar. 2008, available at http://www.usdoj.gov/oig/special/s0803a/final.pdf. For more recent statistics regarding the use of both § 215 requests and § 206 roving wiretap authority, see *Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the S. Judiciary Comm.*, 111th Cong. (Sept. 23, 2009) (written testimony of David Kris, Assistant Attorney General, U.S. Department of Justice).

report indicates that the FBI withdrew at least one such request because the FISC had indicated that it would not sign the order due to First Amendment concerns.[96]

The report identified several issues related to the implementation of § 215 for Congress' consideration. For example, it noted that no settled procedure governs situations in which providers, in response to a § 215 request for documents, submit information that is outside of the scope of the § 215 order. It also stated that in at least one instance, the FBI had issued a national security letter to obtain the same information that had been the subject of a § 215 request that was withdrawn due to First Amendment concerns.[97] It also concluded that the interim minimization procedures, promulgated by the Justice Department to fulfill a requirement that it implement rules to limit the government's acquisition and dissemination of information involving United States citizens, were inadequate.[98]

Effect of Sunset Provisions

As mentioned, the expiring FISA amendments were originally scheduled to sunset on December 31, 2005,[99] but the sunset date for each was extended to December 31, 2009.[100] If that date passed without reauthorization, the amended FISA authorities would read as they did before the enactment of the amendments. For example, regarding roving wiretaps, § 105(c)(2) of FISA would read as it did on October 25, 2001,[101] eliminating the authority for FISA court orders to direct other unspecified persons to assist with electronic surveillance.[102] Likewise, regarding FISA orders for the production of documents, §§ 501 and 502 of FISA would read as they did on October 25, 2001,[103] 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."[104]

However, a grandfather clause applies to each of the three provisions.[105] The grandfather clauses authorize the continued effect of the amendments with respect to investigations that began, or

---

[96] *Id.* at 33. In indicating that it would deny the application, the FISC appears to have decided that "the facts were too 'thin' and that this request implicated the target's First Amendment rights." *Id.* at 68.

[97] *Id.* at 5.

[98] *Id.* at 6.

[99] P.L. 108-458, § 6001(b); P.L. 107-56, § 224(a).

[100] P.L. 109-177, § 103.

[101] 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).

[102] The sunset will not repeal the provision of FISA that permits a FISA warrant to fail to identify 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.

[103] 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).

[104] 50 U.S.C. § 1862(b)(2)(B) (2001).

[105] The 2005 reauthorization act and other measures did not affect the grandfather provisions.

potential offenses that took place, before the provision's sunset date.[106] Thus, for example, if an individual were engaged in international terrorism on December 30, 2009, 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 on December 30, 2009, he may be the target of a roving wiretap under FISA even after authority for new roving wiretaps has expired.

Proposed Legislation in the 111th Congress

Several bills introduced in the 111th Congress would extend all three of the expiring FISA amendments. S. 1692, a bill reported favorably by the Senate Judiciary Committee with an amendment in the nature of a substitute on October 13, 2009, would extend them for four years, creating a new sunset date of December 31, 2013.[107] Examples of other bills that would extend all three amendments include H.R. 1467, which would extend the sunset until December 31, 2019,[108] and S. 1686, which would repeal the sunset provisions.[109]

An alternative proposal introduced in the House, H.R. 3845, would extend the roving wiretap and § 215 amendments but would allow the lone wolf provision to expire.[110] This approach might be prompted in part by indications that the "lone wolf" provision has not yet been relied upon in an investigation.[111]

Some bills propose changes to existing authorities.[112] S. 1692 would alter neither the lone wolf nor the roving wiretap amendments now in effect. However, for the production of documents, it would lower the standard that must be met in an application for a court order. Rather than a "statement of facts showing" that things sought are relevant to an authorized investigation, as is currently required, it would authorize a court order based on a "statement of the facts and circumstances relied upon to justify the belief" that the documents are relevant to such an investigation. However, the bill would preserve the existing standard for library and bookstore records. In contrast, H.R. 3845 would impose a higher standard than is currently in effect, requiring a "statement of specific and articulable facts," rather than a mere "statement of facts," to show that documents or other tangible things sought are relevant to a foreign intelligence investigation. It would also remove the one-year time bar on judicial review of nondisclosure orders associated with FISA court orders for the production of documents. In addition, it would ban the production of library and bookstore records sought "with either the purpose or effect of searching for, or seizing from, a bookseller or library documentary materials that contain personally identifiable information concerning a patron of a bookseller or library." Both bills retain the second part of the amended standard, relevance to an authorized investigation, rather than require a showing that the person to whom the records pertain is a foreign power or its agent, as would be required if § 215 were to expire.

---

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

[107] USA PATRIOT Act Sunset Extension Act of 2009, S. 1692, 111th Cong. (2009).

[108] Safe and Secure America Act of 2009, H.R. 1467, 111th Cong. (2009).

[109] Judicious Use of Surveillance Tools In Counterterrorism Efforts Act of 2009, S. 1686, 111th Cong. (2009).

[110] USA PATRIOT Amendments Act of 2009, H.R. 3845, 111th Cong. (2009).

[111] *See* Letter from the U.S. Department of Justice to Hon. Patrick J. Leahy, at 5 (Sept. 14, 2009).

[112] In contrast, H.R. 1467 would make no changes to the provisions.

H.R. 3845 would also narrow somewhat the circumstances in which the FISC may approve a roving wiretap. It would require that the "identity or description of the specific target of electronic surveillance included in the application ... is sufficient to allow the judge to determine that the target is a single individual."

S. 1692, S. 1686, H.R. 3845, and other bills would modify statutory authorities pertaining to national security letters. S. 1692 and H.R. 3845 would make various authorities for national security letters subject to a December 31, 2013 sunset date, which would mirror the sunset for the expiring amendments to FISA.

Author Contact Information

Anna C. Henning
Legislative Attorney
ahenning@crs.loc.gov, 7-4067

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