Congressional Research Service
Informing the legislative debate since 1914

Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization in Brief

Edward C. Liu
Legislative Attorney

Charles Doyle
Senior Specialist in American Public Law

May 19, 2015

Congressional Research Service
7-5700
www.crs.gov
R44042

CRS REPORT
Prepared for Members and Committees of Congress

Summary

This is an abbreviated version of an earlier report, CRS Report R40980, *Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization*. Both discuss the legal background associated with the sunset of various provisions of the USA PATRIOT Act and of subsequent related legislation, although neither report seeks to track contemporary legislative developments.

Congress enacted the USA PATRIOT Act soon after the 9/11 terrorist attacks. The most controversial sections of the act facilitate the federal government's collection of more information, from a greater number of sources, than had previously been authorized in criminal or foreign intelligence investigations. The Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA), and the national security letter (NSL) statutes were all bolstered. With the changes came greater access to records showing an individual's spending and communication patterns as well as increased authority to intercept email and telephone conversations and to search homes and businesses. In some cases, evidentiary standards required to obtain court approval for the collection of information were lowered. Other approaches included expanding the scope of information subject to search, adding flexibility to the methods by which information could be collected, and broadening the purposes for which information may be sought.

Some perceived the changes as necessary to unearth terrorist cells and update investigative authorities to respond to the new technologies and characteristics of ever-shifting threats. Others argued that authorities granted by the USA PATRIOT Act and subsequent measures could unnecessarily undermine constitutional rights over time. In response to such concerns, sunset provisions were established for many of the changes.

Subsequent legislation made most of these changes permanent. However, a number of authorities affecting the collection of foreign intelligence information are still temporary. For example, subsequent legislation set June 1, 2015, as the expiration date for three such provisions (the lone wolf, roving wiretap, and business record sections of FISA). Additionally, provisions added by the FISA Amendments Act of 2008, relating to the use of foreign intelligence tools to target individuals while they are reasonably believed to be abroad, will expire on December 31, 2017.

Contents

Contacts

Introduction

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."[1] To that end, the act eased restrictions on the government's ability to collect information regarding people's activities and communications, both in domestic criminal investigations and in the realms of foreign intelligence gathering and national security. The changes are perceived by many to be necessary in light of the new breed of threats in a post-9/11 world.[2] The expanded authorities also prompted concerns regarding the appropriate balance between national security interests and civil liberties.[3] In part for that reason, the some of the changes have been revisited and modified in subsequent measures.[4] At this writing, Congress faces the prospect of three provisions expiring this summer and another at the end of 2017.[5]

Constitutional Limitations

To paraphrase the Supreme Court, "the power to secure needed information ... has long been treated as an attribute of the power to" govern.[6] The Constitution, however, particularly the First and Fourth Amendments, limits the manner in which the federal government may collect information.

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."[7] Thus, the Fourth Amendment ultimately limits the government's ability to conduct a range of activities, such as physical searches of homes or offices and listening to phone conversations.[8] As a general rule, the Fourth Amendment requires the government to demonstrate "probable cause" and obtain a warrant

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

[2] *See, e.g.*, *Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the S. Judiciary Comm.*, 111th Cong. (September 23, 2009) (statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers and former Ass't Atty'y Gen. for National Security).

[3] *See, e.g.*, *Unchecked National Security Letter Powers and Our Civil Liberties: Hearing Before the House Perm. Select Comm. on Intelligence*, 110th Cong. (March 28, 2007) (statement of Lisa Graves, then Deputy Director, Center for National Security Studies).

[4] *See, e.g.*, USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177; An act to amend the USA PATRIOT Act to extend the sunset of certain provisions of that act to July 1, 2006, P.L. 109-160; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, P.L. 109-178; Protect America Act of 2007, P.L. 110-55; FISA Amendments Act of 2008, P.L. 110-261.

[5] A pair of historical CRS Reports discuss the individual features of these expiring provisions in greater detail; see CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, and CRS Report R42725, *Reauthorization of the FISA Amendments Act*, both by Edward C. Liu.

[6] McGrain v. Daugherty, 273 U.S. 135, 161 (1927). *McGrain* dealt with the congressional power to gather information in order to legislate prudently.

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

[8] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001); Katz v. United States, 389 U.S. 347, 353 (1967).

(unless a recognized warrant exception applies) before conducting a search.[9] This rule applies most clearly in criminal investigations. For example, an officer conducting a criminal investigation typically may not search a person's belongings without first obtaining a warrant that describes the property for which sufficient evidence justifies a search. But a subpoena is not a warrant, and the Supreme Court some time ago concluded that the government's reasonable collection of information by administrative and grand jury subpoena does not offend the Fourth Amendment, even in the absence of probable cause.[10]

What is Fourth Amendment reasonable in a national security context is less clear. In the 1972 *Keith* case, 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.[11] In contrast with its rulings on surveillance, the Supreme Court has not historically applied the protections of the Fourth Amendment to an individual's documents held by third parties. In 1976, it held that an individual's financial records in the possession of a bank could be obtained by the government with a subpoena.[12] Later, it held that the installation and use of a pen register—a device used to capture telephone numbers dialed—does not constitute a Fourth Amendment search.[13]

First Amendment

The First Amendment restricts government efforts to prohibit the free exercise of religion or to abridge free speech, freedom of the press, the right to peaceful assembly, or the right to petition for redress of grievances.[14] Two First Amendment concerns arise with regard to electronic surveillance, access to records, and related investigatory activities. One addresses direct restrictions on speech that may accompany government collection of private information, such as non-disclosure requirements accompanying orders compelling government access to business records, discussed *infra*. A second concern is that overly broad authorities permitting government intrusion may lead to a "chilling" (i.e., stifling) effect on public discourse.[15] Some post-9/11 laws

[9] *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, for issuance of a search warrant, probable cause requires an issuing magistrate to determine, based on specific evidence, whether there exists a "fair probability" that, for example, an area contains contraband. *Id.* at 238. Exceptions to the warrant requirement include, for example, "exigent circumstances" where people's lives are at risk or illegal items in "plain view" during a search authorized for other items.

[10] Oklahoma Press Pub. Co. v. Walling, 327 US. 186, 195 (1946) (administrative subpoenas); United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991) (citing Hale v. Henkel, 201 U.S. 43, 65 (1906)) (grand jury subpoenas).

[11] United States v. U.S. District Court, 407 U.S. 297, 313-14, 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). *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 of the United States qualifies for the "special needs" exception to the warrant requirement).

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

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

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

[15] *See U.S. District Court*, 407 U.S. at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.").

address the latter issue directly, for example by prohibiting investigations based solely on a person's First Amendment activities.[16] Despite safeguards, there is concern that post-9/11 authorities may have been used to circumvent First Amendment limitations on analogous authorities.[17]

Early Congressional Action

Congress addressed the federal government's access to private information following key Supreme Court decisions interpreting the Fourth Amendment. In 1968, it enacted the predecessor to the Electronic Communications Privacy Act (ECPA), which outlawed the unauthorized interception of wire or oral communications and authorized interception under court supervision for law enforcement purposes.[18] Later, it passed ECPA, which extended protections and authorizations to electronic as well as wire and oral communications.[19]

On the national security side, following the *Keith* case, Congress enacted the Foreign Intelligence Surveillance Act (FISA),[20] in 1976, to create a statutory framework for the use of electronic surveillance to collect foreign intelligence information under the auspice of a special court, the Foreign Intelligence Surveillance Court. Congress subsequently enlarged FISA to include court-supervised use of physical searches, pen registers, and access to certain business records.[21] Similarly, in response to the Supreme Court's rulings regarding the Fourth Amendment's non-application to documents held by third parties, and administrative subpoenas, Congress enacted a series of national security letter (NSL) statutes which, in certain national security cases, afford the federal government access to records held by communications providers, financial institutions, and consumer credit entities.[22]

Changes Made by the USA PATRIOT Act and Subsequent Measures

The USA PATRIOT Act and subsequent measures made far-reaching changes expanding the government's authority to collect private information pursuant to FISA, ECPA, and the NSL

[16] *See, e.g.*, 50 U.S.C. §1842(c).

[17] *See, e.g.*, Office of the Inspector General, Department of Justice, *A Review of the FBI's Use of Section 215 Orders for Business Records in 2006*, March 2008, http://www.usdoj.gov/oig/special/s0803a/final.pdf, at 5 (expressing concern that the FBI had issued a national security letter after the FISA court had twice declined to grant an order for the same material due to First Amendment objections).

[18] P.L. 90-351, 18 U.S.C. §§2510-2520 (1970 ed. Supp. IV).

[19] P.L. 99-508, 18 U.S.C. §§2510-2520 (1988 ed. Supp. II).

[20] P.L. 95-511, §807(a)(3)(1994), 50 U.S.C. §1821 *et seq*. (physical search orders); P.L. 105-272, §601, 602 (1998), 50 U.S.C. §1841 *et seq*. (pen register orders); P.L. 105-272, §602 (1998), 50 U.S.C. §1861 *et seq*. (2000 ed.)(business record orders). Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of an incoming call on a particular phone line. *See* 18 U.S.C. §3127(3)-(4).

[21] P.L. 103-359, §807(a)(3), 50 U.S.C. §§1821-1829.

[22] Electronic Communications Privacy Act, P.L. 99-508, §201(a), 18 U.S.C. §2709 (communications providers); P.L. 99-569, §404, 12 U.S.C. §3414(a)(5)(A) (financial institutions); P.L. 104-93, §601(a), 15 U.S.C. 1681u (consumer credit entities).

statutes.[23] The legislation scheduled three of the FISA amendments—the lone wolf, roving wiretap, and business record provisions—to expire on June 1, 2015.

Lowering of the Wall Between Criminal Investigations and Foreign Intelligence Gathering

The USA PATRIOT Act lowered somewhat the wall traditionally separating criminal investigation from foreign intelligence gathering. Prior to the act, FISA required that foreign intelligence gathering be the sole or primary purpose of an investigation; thus, activities conducted with an additional rationale of criminal investigation were required to adhere to criminal procedure requirements. Section 218 of the act amended the standard to require that foreign intelligence gathering be a "significant" rather than "the [sole]" purpose of surveillance or a search for which a court order is sought under FISA.[24] Thus, the presence of ancillary criminal investigation purposes no longer eliminates the ability to rely on FISA authorities, so long as a significant foreign intelligence purpose also exists.

The act also attempted to improve communication between foreign intelligence and criminal law enforcement agencies. To that end, it includes several provisions that authorize information sharing. For example, section 504 authorizes federal officers to consult with criminal law enforcement officers regarding information obtained from a physical search in order "to coordinate efforts to investigate or protect against" various national security threats.[25]

Expansion of Persons Subject to Investigation

Several post-9/11 measures addressed threshold or definitional issues affecting the range of persons whose communications, records, or effects might be investigated as part of foreign intelligence gathering. The controversial 2004 lone wolf provision, one of the three expiring provisions, is especially significant. It expanded the definition of "agent of a foreign power" in FISA to include a non-U.S. person who "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power."[26] Because FISA orders—including those for surveillance, physical searches, pen registers, trap and trace devices, and business records—require evidence indicating that a target is a foreign power or its agent, the broadened definition makes the authorities applicable to targets for which a link to an international terrorist organization or other foreign power is not yet supported by probable cause.[27]

---

[23] Expansions were also made to some related authorities. For example, the USA PATRIOT Act and subsequent legislation amended the grand jury secrecy rule to permit prosecutors to disclose grand jury information to federal, state, local, or foreign law enforcement or intelligence officials under certain circumstances.

[24] 50 U.S.C. §1804(a)(7)(B) (electronic surveillance); 50 U.S.C. §1823(a)(7)(B) (physical searches).

[25] 50 U.S.C. §1806(k)(1) (electronic surveillance); 50 U.S.C. §1825 (physical searches).

[26] *Id*. at §6001(a); 50 U.S.C. §1801(b)(1)(C).

[27] *But see* Letter from Assistant Attorney General Ronald Weich to Hon. Patrick J. Leahy, at 5 (September 14, 2009), http://judiciary.senate.gov/resources/documents/111thCongress/upload/091409WeichtoLeahy.pdf (indicating that the lone wolf provision has not yet been relied upon in a federal investigation). For more information regarding the lone wolf provision and the other expiring amendments to FISA, see CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended Until June 1, 2015*, by Edward C. Liu.

Another important expansion followed in the wake of revelations regarding the Terrorist Surveillance Program. Two measures, discussed in greater detail *infra*,[28] eased federal officials' ability to gather foreign intelligence information between persons in the United States and others thought to be located outside of the United States. In the first, now expired, measure, Congress exempted "surveillance directed at a person reasonably believed to be located outside of the United States" from the definition of "electronic surveillance" under FISA.[29] Although this made it unnecessary to obtain a FISA order to conduct such surveillance, Congress simultaneously established temporary procedures governing the capture of communications for specified groups of targets reasonably believed to be located overseas.[30] The second measure provides separate authorities with differing standards for targeting non-U.S. persons and U.S. persons reasonably believed to be located outside the United States.[31]

Finally, by authorizing the collection of information believed to be *relevant to* a national security or foreign intelligence investigation, the USA PATRIOT Act and its successors in several instances widened the circle of persons whose communications or effects might fall within the ambit of authorities for intelligence gathering.[32] Authorities had previously limited that circle to persons believed to be agents of foreign powers.

Expansion of Electronic Surveillance Authorities

The USA PATRIOT Act and its progeny made several changes to FISA's electronic surveillance authorities. The so-called "roving wiretap" provision, section 206 of the USA PATRIOT Act, permits roving or multipoint wiretaps where the Foreign Intelligence Surveillance Court finds that the actions of the target of the application for electronic surveillance under FISA may have the effect of thwarting the identification of a specific communications or other common carrier, landlord, custodian, or specified person to whom the order to furnish information, facilities, or technical assistance in connection with the wiretap should be directed.[33] As amended by P.L. 109-177, this finding must be based upon specific facts provided in the application.[34] In addition, section 207 of the USA PATRIOT Act extended the duration of FISA wiretaps and extensions thereof.[35]

Section 225 added a new provision to FISA that bars suits against any wire or electronic service provider, custodian, landlord, or other person that furnishes information, facilities, or technical assistance in connection with electronic surveillance pursuant to a FISC order or with a request for emergency assistance under FISA.[36]

---

[28] *See* discussion regarding the aftermath of the Terrorist Surveillance Program.

[29] The Protect America Act of 2007, P.L. 110-55.

[30] *Id.*

[31] The FISA Amendments Act of 2008, P.L. 110-261.

[32] *See, e.g.*, P.L. 109-177, §106(b), 50 U.S.C. §§1861-1863; P.L. 107-56, §505(a)(3), 18 U.S.C. §2709.

[33] 50 U.S.C. §1805(c)(2)(B).

[34] *Id.*

[35] P.L. 107-56, §207, 50 U.S.C. §1805(e).

[36] P.L. 107-56, §225, 50 U.S.C. §1805(i). This section was expanded by section 314(a)(2)(D) of the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, to cover those who provide such assistance in connection with a FISA order authorizing a physical search or emergency assistance.

Expansion of Authorities to Conduct Physical Searches

"Physical searches," as defined by FISA, are analogous to searches authorized by warrants in criminal investigations.[37] The most notable amendment specific to FISA provisions governing orders for physical searches, made by section 207 of the USA PATRIOT Act, increased the maximum duration of physical search orders targeting persons other than a foreign power.[38] The maximum duration of such orders was 45 days but is now 120 days for searches targeting an agent of a foreign power and 90 days for other targets.[39]

Expansion of Authorities for Pen Registers and Trap and Trace Devices

The USA PATRIOT Act amended both FISA provisions relevant to the use of pen register and trap and trace devices. The most notable amendment to FISA was made in section 214. Previously, the use of pen registers and similar devices could be authorized only for investigations to gather foreign intelligence information or information concerning international terrorism. Section 214 broadened the purposes for which the devices may be authorized by allowing their use in "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[40] However, it prohibits any investigation involving a U.S. person that is "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[41]

Expanded Access to Records and Other Tangible Things

As mentioned, the USA PATRIOT Act focused in part on the statutory tools available in anti-terrorism investigations. Some of those tools enable agents to unearth documents that reveal the paper trail of crime and of the activities of international terrorist organizations and other foreign powers and their agents—grand jury, administrative, and judicial subpoenas; search warrants; court orders under the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA); and national security letters (NSLs). The most important changes were made to FISA and the national security letter statutes. The USA PATRIOT Act and the related legislation that followed sought to make those implements more effective within a system of reinforced civil liberties safeguards.

---

[37] The definition of "physical search" in FISA incorporates the standard—"reasonable expectation of privacy"—which typically triggers the Fourth Amendment warrant requirement in criminal investigations. *See* 50 U.S.C. §1821(5) (defining "physical search" as "any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, *under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes*, but does not include (A) "electronic surveillance" ... or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law.... ") (emphasis added).

[38] P.L. 107-56, §207, 50 U.S.C. §1824(d). The maximum duration of a physical search order targeting a foreign power was and is one year.

[39] *Id*.

[40] P.L. 107-56, §214, 50 U.S.C. §1842(a)(1).

[41] *Id*.

National Security Letters

The USA PATRIOT Act expanded authorities for agency-issued national security letters. It authorized their issuance with the approval of the Special Agents in Charge of FBI field offices (SACs); broadened the range of permissible targets; and enacted the community-wide-all-consumer credit-information national security letter statute.[42] Prior to the USA PATRIOT Act, the national security letter statutes permitted issuance only upon government certification of specific and articulable facts, giving reason to believe that the information sought pertained to a foreign power or one of its agents.[43] Now, they require a certification that the information is relevant to, or is sought for, a particular national security investigation.[44] The change means that national security letters may be issued at a stage in the investigation when the precise relationship (if any) of a subject to a specific terrorist organization or other foreign power has yet to be established. It also means that information is more likely to be gathered from people several steps removed from a foreign power or its agents and is more likely to pertain to individuals not ultimately of interest.

Reports of the inspector general of the Department of Justice indicate that the FBI previously did not find pre-amendment national security letters particularly useful but now considers them indispensable.[45] Information gleaned from national security letter responses is used to produce analytical intelligence reports; further investigations; provide the basis for FISA orders and pursue other investigative techniques; and help decide whether to open, continue, or close an investigation or line of inquiry.[46] However, the inspector general also found that, at least initially, "the FBI used national security letters in violation of applicable national security letter statutes, Attorney General Guidelines, and internal FBI policies."[47]

FISA Orders for Business Records and Other Tangible Things

Section 215 of the USA PATRIOT Act, one of the three amendments to FISA scheduled to expire on June 1, 2015, was perhaps the act's most controversial provision. It expanded the authority for FISA orders compelling records and other tangible things in two ways. First, it enlarged the scope of materials that may be sought. Prior to the enactment of the USA PATRIOT Act, FISA authorized court orders for access to only four types of business records: car rental records, housing accommodation (e.g., hotel/motel) records, storage rental records, and travel (e.g., airline/train) records.[48] As amended, the section authorizes the FISC to issue orders for access to "any tangible things."[49] Second, the section lowered the standard which must be met before the

[42] P.L. 107-56, §§328(g), 505.

[43] *See, e.g.,* 18 U.S.C. §2709 (2000 ed.). A textual comparison of the NSL statutes now and prior to the USA PATRIOT Act appears as an appendix in CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background*, by Charles Doyle.

[44] *See, e.g.*, 18 U.S.C. §2709.

[45] Office of the Inspector General, U.S. Department of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007) (*IG Rept. I)* at 43-5; Office of the Inspector General, U.S. Department of Justice, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2008) (*IG Rept. II)* at 114-16.

[46] *IG Rept. I* at 46.

[47] *Id.* at 124. Second IG's report indicated it was too soon to tell whether the FBI had eliminated the problems identified in the first report, *IG Rept. II* at 161.

[48] 50 U.S.C. §§1861-1862 (2000 ed.).

[49] 50 U.S.C. §1861(a)(1).

court may issue such orders. The previous standard required a showing of specific and articulable facts giving reason to believe the information related to a foreign power or the agent of a foreign power. As amended, the provision now requires "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.]"[50]

Specific concerns regarding the provision's potential application to library records and other materials thought to be particularly private or sensitive prompted further revisions to the relevant FISA authorities. In 2006, Congress modified the tangible item provisions to restrict the officials who may apply for orders covering library, bookstore, gun sale, tax or medical records to senior FBI headquarters officials; for other types of materials, FBI field office SACs may also apply.[51]

The 2006 measures also called for audits of the use of section 215 authority by the Justice Department's inspector general.[52] The resulting reports indicate that the authority was exercised only relatively infrequently and most often in part to secure information that is now available under FISA trap and trace authority.[53] Prior to the 2006 amendments, FISA trap and trace authority did not permit the order to include a demand for related customer record information, a problem authorities overcame by submitting a FISA tangible item order request in combination with a FISA trap and trace order request.[54] The 2006 amendments enlarged FISA trap and trace authority so that such "combo" FISA applications are no longer necessary.[55] The FISA court approved six "pure" section 215 requests in 2004; 14 in 2005; 15 in 2006; 17 in 2007; and 18 in 2008.[56] The IG reports suggest several reasons for the sparse use. The approval process is less familiar, multi-layered, sometimes cumbersome, and time consuming.[57] Moreover, voluntary compliance, NSLs, grand jury subpoenas, or FISA trap and trace orders can often provide access to the same documents more quickly.[58] Nevertheless, the Justice Department considers section 215 authority to be a valuable tool when these alternative means are not available.[59]

A final important change affected the burden of proof for the standard of relevancy. Record checks are often the "stuff" of running down leads. Before 2006, FISA tangible-item orders were available when "sought" for certain national security investigations—that is, sometimes to determine whether they would be relevant, not because they were determined to be relevant.[60] In such cases, FISA responses not infrequently included irrelevant information. After the 2006 amendments, the orders authorize government access only to relevant information.[61] However,

---

[50] 50 U.S.C. §§1861-1863.

[51] 50 U.S.C. §1861(a).

[52] P.L. 109-177, §§102(b), 106A.

[53] Office of the Inspector General, U.S. Department of Justice, *A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records* (March 2007) (*IG 215 Rept. I*); Office of the Inspector General, U.S. Department of Justice, *A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records in 2006* (March 2008) (*IG 215 Rept. II*).

[54] *IG 215 Rept.I* at 16-7.

[55] *Id.* at 17; 50 U.S.C. §1842(d)(2)(C).

[56] *IG 215 Rept. I* at 17; *IG 215 Rept. II* at 15.

[57] *IG 215 Rept. II* at 57.

[58] *Id*.

[59] *Id.* at 58.

[60] 50 U.S.C. §1861(b) (2000 ed., Supp. I).

[61] 50 U.S.C. §1861(b).

records are declared "presumptively relevant" if they pertain to a foreign power or one of its agents, to the suspected agent who is the subject of the investigation, or to an individual in contact with, or known to, such an agent.[62] The relevancy presumption seems to make acquisition of information pertaining to "innocent" Americans more likely. Foreign agents may "know" many people, some involved in their nefarious activities, others not. The amendment creates a presumption of relevancy for information pertaining to both groups.

Judicial Oversight and Minimization Procedures

Congress relies on three types of safeguards to protect against abuse of the new authority established by the USA PATRIOT Act and its successors: congressional oversight, judicial oversight, and minimization procedures.

Congressional Oversight

Measures following the USA PATRIOT Act established various reporting and notification requirements, presumably to provide transparency regarding the use of enhanced authorities. For example, section 6002 of the FISA Amendments Act of 2004, P.L. 108-458, requires the Attorney General, on a semiannual basis, to report to relevant committees regarding the use of various FISA authorities, Foreign Intelligence Surveillance Court decisions, and related matters for each preceding six-month period.[63]

Congress instituted additional reporting requirements when it reauthorized and made permanent many USA PATRIOT Act provisions in 2005. For example, section 114 of the USA PATRIOT Improvement and Reauthorization Act of 2005 enhanced congressional oversight of delayed notice search warrants by requiring that no later than 30 days after the expiration or denial of such a warrant, the issuing or denying judge notify the Administrative Office of the U.S. Courts of (1) an application for a delayed notice search warrant; (2) whether the warrant was either granted, modified, or denied; (3) the length of time of the delay in giving notice; and (4) the offense specified in the warrant or the application.[64] In addition, it requires the Director of the Administrative Office to submit an annual report to Congress summarizing the use of delayed notice warrants.[65]

Similarly, section 209 of the 2005 reauthorization measure instituted a semi-annual reporting requirement, whereby the Attorney General must report to the Senate Judiciary Committee and the House and Senate Intelligence Committees regarding physical searches conducted pursuant to FISA, and must submit to those committees and the House Judiciary Committee a report with statistical information concerning the number of emergency physical search orders authorized or denied by the Attorney General.[66] Likewise, section 128 requires that the Judiciary Committees

[62] 50 U.S.C. §1861(b)(2).

[63] P.L. 108-458, §6002, 50 U.S.C. 1801 note.

[64] P.L. 109-177, §114, 18 U.S.C. §3103a(d)(1).

[65] *Id*.

[66] P.L. 109-177, §109(a), 50 U.S.C. §1826.

receive full reports on the use of the FISA's pen register and trap and trace authority every six months.[67]

Judicial Oversight

Notification requirements facilitate judicial oversight as well. For example, section 216 of the USA PATRIOT Act requires law enforcement officers to submit a detailed report to the court authorizing the search describing information collected via pen registers and trap and trace devices.[68] The requirement was likely a response to objections that email header information, now authorized to be collected, can be more revealing than a telephone number.

Congress and the courts have also addressed individuals' direct access to judicial review. For example, section 223 of the USA PATRIOT Act amended ECPA to authorize a cause of action against the United States for willful violation by federal employees of the stored communications and records provisions, of the court-ordered interception provisions, and of the FISA electronic surveillance, physical search, pen register, or trap and trace device provisions.[69]

The federal courts have in some cases determined that insufficient access to judicial review raises constitutional problems. In the context of national security letters, the U.S. Court of Appeals for the Second Circuit, in *John Doe, Inc. v. Mukasey*,[70] held that the current gag order and accompanying judicial review provisions only survive First Amendment scrutiny if the government takes specified actions. Namely, it must promptly petition for judicial review (at the recipient's option) and convince the district court that the proposed secrecy provision is narrowly crafted to meet the statutorily identified adverse consequences of disclosure.[71] The *John Doe, Inc.* court also found unconstitutional the statutory requirement (18 U.S.C. §3511(b)) that a reviewing court give conclusive weight to the government's certification that disclosure might have adverse consequences.[72]

Judicial review of nondisclosure orders accompanying FISA tangible items orders would seem to stand on different footing. The First Amendment defect in the NSL provisions is the want of prompt judicial involvement. The nondisclosure orders under FISA are issued by the FISC, a neutral judicial body, and consequently would seem to suffer no such malady. The statute, however, establishes an intricate procedure under which a recipient must wait a year before filing

[67] P.L. 109-177, §128(b), 50 U.S.C. §1846(a).

[68] P.L. 107-56, §216, 18 U.S.C. §3123(a)(3).

[69] P.L. 107-56, §223(c), 18 U.S.C. §§2510(19), 2712.

[70] 549 F.3d 861 (2d. Cir. 2008). The Second Circuit also held that that Section 215 did not authorize the National Security Agency's bulk metadata collection program. American Civil Liberties Union v. Clapper, ___ F.3d ___, ___ *33 (2d Cir. May 7, 2015); see generally, CRS Legal Sidebar, *The Potential Impact of the Second Circuit's Ruling Against Bulk Collection on USA PATRIOT Act Reauthorization*, by Edward C. Liu.

[71] For national security letters, such consequences include danger to the national security or to individual safety, or interference with diplomatic relations or with a criminal counter-intelligence, or counter-terrorism investigation. In a criminal context, disclosure of an officer's purpose to execute a warrant may be excused if disclosure is likely to result in adverse consequences such as the loss of evidence, flight of a suspect, or a danger to individual safety, Wilson v. Arkansas, 514 U.S. 927, 935-36 (1995).

[72] *Mukasey*, 549 F.3d at 883. A district court in the Ninth Circuit also concluded that the NSL nondisclosure and judicial review provisions were constitutionally suspect. Although the district court refused to enclose the "fix" described in *John Doe, Inc*., it stayed its final order pending appeal. In re National Security Letter, 930 F. Supp. 2d 1064, 1081 (N.D.Cal. 2013).

a motion to modify or set aside a nondisclosure requirement.[73] Petitions, which survive a screening process designed to weed out frivolous challenges, may be granted only if the judge concludes that there is no reason to believe that disclosure would endanger national security or individual safety or would interfere with a diplomatic relations or a criminal, counter-terrorism, or counter-intelligence investigation.[74] As in the NSL statute provision to which the Second Circuit objected,[75] the government's certification of a possible adverse impact on national security or diplomatic relations is conclusive.[76] If a petition is denied, a renewed petition may not be filed until a year later.[77]

Although FISA does not say so in so many words, the recipient of a FISA order who disobeys an order of the court probably stands in contempt of court.[78] It may be assumed that FISA court-issued orders would be beyond reproach on First Amendment grounds when issued. Yet, the time bars on release from a gag order for which the need has passed might be thought troubling. The time bars notwithstanding, however, a recipient might find an effective avenue for timely review by refusing to comply with the order to produce followed by a challenge to the gag order at the subsequent show cause or habeas hearing.

Minimization Procedures

Minimization means different things in different contexts. In an abstract sense, it means capturing, keeping, using, and passing on to others no more information than is necessary to satisfy the purposes for which the statutory authority to do so was given. Under ECPA, it means procedures to minimize the interception of communications other than those for which the Title III order was granted.[79] Under FISA, minimization means, roughly, procedures to curtail the interception of the communications of Americans consistent with national security needs.[80] FISA also has provisions governing the use of FISA-generated evidence in subsequent federal or state proceedings under which district courts may review the legality of the use of FISA authority and suppress the resulting evidence when appropriate.[81]

Today, the national security letter statutes have no comparable provisions, although most have dissemination limits.[82] Section 119 of the USA PATRIOT Improvement and Reauthorization Act of 2005 directed the Attorney General to report on the feasibility of establishing national security letter minimization procedures.[83] A report prepared by the Justice Department's inspector general discussed efforts of the Justice Department to formulate such procedures and reservations

[73] 50 U.S.C. §1861(f).

[74] 50 U.S.C. §1861(f)(2).

[75] 549 F.3d 861, 882-83 (2d Cir. 2008) ("the fiat of a governmental official, though senior in rank and doubtless honorable in the execution of official duties, cannot displace the judicial obligation to enforce constitutional requirements").

[76] 50 U.S.C. §1861(f)(2)(C)(ii).

[77] 50 U.S.C. §1861(f)(2)(C)(iii).

[78] *Cf.*, 18 U.S.C. §§401, 402.

[79] 18 U.S.C. §2518(5).

[80] 50 U.S.C. §1801(h).

[81] 50 U.S.C. §§1806, 1825.

[82] 18 U.S.C. §2709(d); 12 U.S.C. §3414(a)(5)(B); 15 U.S.C. §1681u(f); 50 U.S.C. §436(e).

[83] P.L. 109-177, §119(f).

concerning the initial proposals.[84] The inspector general has also testified that such procedures are needed and overdue, but acknowledged that the task has proven challenging.[85] He expressed the view that the national security letter minimization procedures should address "collection of information through national security letters, how the FBI can upload national security information in FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of national security letter derived information in FBI databases and files, and the time period for retention of national security letter obtained information."[86]

Unlike the NSL statutes, section 215 of the USA PATRIOT Act, as amended, has an explicit minimization component, which calls for procedures governing the retention and dissemination of records and other tangible things collected pursuant to FISA orders.[87] The Justice Department, however, failed to reach internal consensus on issues such as "the time period for retention of information, definitional issues of 'U.S. person identifying information,' and whether to include procedures for addressing material received in response to, but beyond the scope of, the FISA Court order; uploading information into FBI databases; and handling large or sensitive data collections."[88] Accordingly, it issued interim procedures, which the inspector general concluded "do not adequately address the intent and requirements of the [law] for minimization requirements."[89]

Conclusion

Arguments raised in the earlier debates reflect fundamental questions regarding the level of government intrusion necessary to ensure the country's safety. Referring to the expiring provisions, the U.S. Department of Justice asserts that the expanded authorities have proven to be important and effective intelligence gathering tools.[90] Thus, although it is "willing to consider" proposals to modify authorities to provide additional privacy protections, the Justice Department warns that care should be taken to ensure that any changes to existing authorities "do not undermine the effectiveness of [the expiring FISA amendments]."[91]

Countervailing arguments assert that amendments enacted following the 9/11 terrorist attacks undermined citizens' civil liberties unnecessarily.[92] Specifically, they argue that the broader the authorities for the collection of foreign intelligence information, the greater the likelihood that U.S. citizens' private conversations or documents will be swept within the scope of an authorized investigation. For example, a concern might be that the authority for "roving wiretaps" increases the likelihood that innocent conversations involving U.S. citizens will be the subject of electronic

[84] *IG Rept. II* at 64-72.

[85] *Reauthorizing the USA Patriot Act: Hearings Before the Senate Comm. on the Judiciary*, 111th Cong. (2009) (statement of U.S. Department of Justice Inspector General Glenn A. Fine).

[86] *Id.*

[87] 50 U.S.C. §1861(g).

[88] *IG 215 Rept. II* at 76.

[89] *Id.* at 87.

[90] Letter from the U.S. Department of Justice to Hon. Patrick J. Leahy (September 14, 2009), http://judiciary.senate.gov/resources/documents/111thCongress/upload/091409WeichtoLeahy.pdf.

[91] *Id*.

[92] *See e.g.*, *Restoring the Rule of Law: Hearing Before the Senate Comm. on the Judiciary, Subcomm. on the Constitution*, 110th Cong. (September 16, 2008) (statement of Suzanne E. Spaulding, Esq.).

surveillance. Likewise, at least one commentator asserts that national security letters have a "too diffuse" focus, which leads to anecdotal evidence showing that "their effectiveness is disproportionately small compared with the extent of ... the invasion of privacy they represent."[93]

Reflecting the arguments on both sides, the legislative debate is likely to address ways in which the need for rigorous investigative tools might be balanced with the safeguarding of constitutional guarantees.

Author Contact Information

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

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968

[93] *Unchecked National Security Letter Powers and Our Civil Liberties: Hearing Before the House Perm. Select Comm. on Intelligence*, 110th Cong. (March 28, 2007) (statement of Lisa Graves, then Deputy Director, Center for National Security Studies).