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

Anna C. Henning, Coordinator
Legislative Attorney

Elizabeth B. Bazan
Legislative Attorney

Charles Doyle
Senior Specialist in American Public Law

Edward C. Liu
Legislative Attorney

December 9, 2009

Congressional Research Service
7-5700
www.crs.gov
R40980

Summary

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 e-mail 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 measures made most of the USA PATRIOT Act changes permanent. However, three authorities affecting the collection of foreign intelligence information are set to expire on December 31, 2009: the lone wolf, roving wiretap, and business record sections of FISA. The impending expiration date has prompted legislative proposals which revisit changes made by the USA PATRIOT Act and related measures. Examples of relevant bills include the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692) and the USA PATRIOT Amendments Act of 2009 (H.R. 3845), which were reported or ordered to be reported from their respective judiciary committees, as well as a number of additional bills, including S. 1686, S. 1725, S. 1726, S. 2336, H.R. 1800, H.R. 3846, H.R. 3969, and H.R. 4005.

In addition to the expiring provisions, pending bills address a range of issues, including national security letters, minimization requirements, nondisclosure requirements (gag orders), interception of international communications, and retroactive repeal of communication provider immunity for Terrorist Surveillance Program (TSP) assistance. This report surveys the legal environment in which the legislative proposals arise.

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 conversations, 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 changes were revisited and modified in subsequent measures.[4]

Several pending legislative proposals would further adjust USA PATRIOT Act provisions and related authorities for the government's collection of private information. Examples of relevant bills include the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692) and the USA PATRIOT Amendments Act of 2009 (H.R. 3845), which were reported or ordered to be reported from their respective judiciary committees.[5]

The current legislative debate is catalyzed, in part, by a sunset date of December 31, 2009, for three amendments which expanded authorities for the collection of foreign intelligence information.[6] However, pending bills cover a range of authorities expanded by the USA PATRIOT Act in addition to the expiring provisions.

This report discusses the history of constitutional interpretations and legislative responses relevant to the collection of private information for criminal investigation, foreign intelligence gathering, and national security purposes. Next, it summarizes the relevant statutory frameworks and changes made by the USA PATRIOT Act and subsequent measures. It then examines congressional oversight, judicial review, and "minimization procedures" designed to limit the

[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. (Sept. 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. (Mar. 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] Additional relevant proposals include, for example, S. 1686, S. 1725, S. 1726, S. 2336, H.R. 1800, H.R. 3846, H.R. 3969, and H.R. 4005.

[6] Although the three expiring provisions are thought of as the "expiring Patriot Act provisions," *see, e.g., Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Hearing Before the Senate Comm. on the Judiciary*, 111th Cong. (Sept. 23, 2009) (statement of Sen. Leahy), only two of the three expiring provisions were enacted in the Patriot Act. *See* P.L. 107-56, § 206, 50 U.S.C. § 1805(c)(2)(B) (known as the "roving wiretap" provision); *Id*. at § 215, 50 U.S.C. §§ 1861-2 (known as the "business records" or "library" provision). The third provision, known as the "lone wolf" provision, is Section 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA). P.L. 108-458, 50 U.S.C. § 1801(b)(1)(C).

extent of government intrusions where possible. Finally, it discusses several related matters likely to play a role in the legislative debate surrounding reauthorization of the expiring provisions.

Constitutional Limitations

Constitutional limitations restrict the government's ability to access private information. The Fourth Amendment to the U.S. Constitution is particularly relevant. To the extent that government activity burdens individuals' freedom of speech and related rights, the First Amendment may also play a role.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution provides a right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[7] Many of the government activities discussed in this report have the potential to constitute a search as that term is defined in Fourth Amendment jurisprudence. Namely, government action constitutes a search when it intrudes upon a person's "reasonable expectation of privacy," which requires both that an "individual manifested a subjective expectation of privacy in the searched object" and that "society is willing to recognize that expectation as reasonable."[8]

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. As a general rule, the Fourth Amendment requires the government to demonstrate "probable cause" and obtain a warrant (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.

The extent to which the Fourth Amendment warrant requirement applies to the government's collection of information for intelligence gathering and other purposes unrelated to criminal investigations is unclear. Although the surveillance of wire or oral communications for criminal law enforcement purposes was held to be subject to the warrant requirement of the Fourth Amendment in 1967,[10] neither the Supreme Court nor Congress sought to regulate the use of such surveillance for national security purposes at that time. Several years later, the Supreme Court invalidated warrantless electronic surveillance of domestic organizations for national security purposes, but indicated that its conclusion might differ if the electronic surveillance targeted

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

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

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

foreign powers or their agents.[11] A lower court has since upheld the statutory scheme governing the gathering of foreign intelligence information against a Fourth Amendment challenge, despite an assumption that orders issued pursuant to the statute might not constitute "warrants" for Fourth Amendment purposes.[12] The Supreme Court has not yet directly addressed the issue. However, even if the warrant requirement was found not to apply to searches for foreign intelligence or national security purposes, such searches would presumably be subject to the general Fourth Amendment "reasonableness" test.[13]

In contrast with its rulings on surveillance, the Supreme Court has not historically applied the protections of the Fourth Amendment to documents held by third parties. In 1976, it held that financial records in the possession of third parties could be obtained by the government without a warrant.[14] Later, it likewise 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.[15] The reasoning was that individuals have a lesser expectation of privacy with regard to information held by third parties.

First Amendment

The First Amendment to the U.S. Constitution 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.[16] 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.[17] Some post-9/11 laws address the latter issue directly, for example by prohibiting investigations based solely on a person's First Amendment activities.[18] Despite safeguards, there

[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 U.S. qualifies for the "special needs" exception to the warrant requirement).

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

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

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

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

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

[17] *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.").

[18] *See, e.g.*, 50 U.S.C. § 1842(c).

is concern that post-9/11 authorities may have been used to circumvent First Amendment limitations on analogous authorities.[19]

History of 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 legislation, Title III of the Omnibus Crime Control and Safe Streets Act, which outlawed the unauthorized interception of wire or oral communications and authorized interception under court supervision for law enforcement purposes.[20] Later, it passed the Electronic Communications Privacy Act (ECPA), which incorporated and modernized Title III to cover electronic as well as wire and oral communications.[21]

In the years following the Supreme Court's 1972 ruling on surveillance (the "*Keith* case"), Congress actively examined the intelligence practices of past presidential administrations and found that every administration since Franklin D. Roosevelt engaged in electronic surveillance without prior judicial approval.[22] It also found that the authority was sometimes abused.[23] Partly in light of these findings, Congress enacted the Foreign Intelligence Surveillance Act (FISA)[24] to create a statutory framework for the use of electronic surveillance to collect foreign intelligence information.

Similarly, in response to the Supreme Court's rulings regarding the Fourth Amendment's non-application to documents held by third parties, Congress enacted the Right to Financial Privacy Act (RFPA)[25] to constrain government authorities' access to individuals' financial records. Although these privacy protections are subject to a foreign intelligence exception,[26] government authorities were not authorized to compel financial institutions to secretly turn over financial records until 1986.[27] That year, the FBI was also given authority, in the form of FBI-issued

[19] *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*, Mar. 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).

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

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

[22] *See* S. Rept. 95-604(I), at 7, 1978 U.S.C.C.A.N. 3904, 3908.

[23] The report of a congressional committee convened to examine intelligence gathering after Watergate stated: "Too many people have been spied upon by too many government agencies and too much information has been collected. The government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone 'bugs', surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens." *See Intelligence Activities and the Rights of Americans, Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities and the Rights of Americans, United States Senate, Book II*, S. Rept. 94-755, at 5 (1976) (hereinafter Church Committee Final Report). *See also Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans, Church Committee Final Report,, Book III*, S. Rept. 94-755, at 271-351.

[24] P.L. 95-511, 50 U.S.C. § 1801 *et seq.*

[25] P.L. 95-630, § 1114, 12 U.S.C. § 3401 *et seq.*

[26] 12 U.S.C. § 3414(a)(1)(A), (B).

[27] P.L. 99-569, § 404, 12 U.S.C. § 3414(a)(5)(A).

"national security letters," to access customer records held by telephone companies and other communications service providers in specified instances justified by a national security rationale.[28] Two additional national security letter authorities were enacted in the mid-1990s. The first provided access to credit and financial records of federal employees with security clearances.[29] The second gave the FBI access to credit agency records in order to facilitate the identification of financial institutions utilized by the target of an investigation.[30]

Intelligence gathering laws were expanded during the same time period. In 1994, FISA was amended to cover physical searches for foreign intelligence purposes.[31] Four years later, Congress amended FISA to permit the Foreign Intelligence Surveillance Court to issue orders authorizing (1) the use of pen registers and trap and trace devices to track calling patterns;[32] and (2) the production of some business records not available through existing national security letter authorities.[33]

The USA PATRIOT Act,[34] enacted in 2001, represented a broad expansion of existing statutory authorities. It eliminated barriers to cooperation between law enforcement and foreign intelligence investigations, modified surveillance authorities under both FISA and ECPA, and created a fifth category of national security letters. Many of these provisions were made temporary, subject to sunset in 2005.[35]

In 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act. Among other things, the Act amended FISA to allow targeting so-called "lone wolves" or individuals believed to be engaged in terrorism, but who were not linked to a known terrorist organization.[36] The "lone wolf" provision was given an expiration date to match that which applied to many of the USA PATRIOT Act provisions.

The next year, Congress reauthorized the USA PATRIOT Act, making the majority of its expiring provisions permanent.[37] However, two of its most controversial provisions, discussed *infra*, together with the 2004 lone wolf provision, were given a new sunset date of December 31, 2009.[38]

Also in 2005, President Bush acknowledged that he had authorized a Terrorist Surveillance Program (TSP), which captured some international communications apparently procured without judicial or statutory authority. As discussed *infra*, Congress subsequently enacted the Protect America Act and the FISA Amendments Act of 2008, which addressed issues raised in response to the TSP.

[28] Electronic Communications Privacy Act, P.L. 99-508, § 201(a), 18 U.S.C. § 2709.

[29] P.L. 103-359, § 802, 50 U.S.C. § 436.

[30] P.L. 104-93, § 601(a), 15 U.S.C. § 1681u.

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

[32] 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).

[33] P.L. 105-272, §§ 601, 602.

[34] P.L. 107-56.

[35] *Id.* at § 224.

[36] P.L. 108-458, § 6001.

[37] P.L. 109-177, § 102(a).

[38] *Id.* at §§ 102(b), 103.

Statutory Framework

The applicable statutory regime or procedural rules differ according to the purpose for which the federal government collects private information. In criminal law enforcement investigations, the Federal Rules of Criminal Procedure, ECPA, and other provisions in Title 18 of the U.S. Code apply. In contrast, the collection of foreign intelligence information is governed by FISA. Finally, five national security statutes, discussed *infra*, regulate the issuance of national security letters. Statutes in these areas provide analogous authorities for various government activities but require that different standards and procedures be satisfied.

Federal Rules of Criminal Procedure and Subpoena Authorities

In criminal cases, federal officials ordinarily gain access to spaces, documents, and other private materials pursuant to a warrant (during investigation) or a subpoena (during prosecution). In criminal investigations, Federal Rule of Criminal Procedure 41 provides procedures applicable to search warrants to obtain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; or property "designed for use, intended for use, or used in committing a crime."[39]

During the indictment phase, federal grand juries have the power to investigate the possibility that a federal crime has been committed within the judicial district in which they are convened and enjoy the benefit of the subpoena power of the court within whose district they sit. [40] However, grand jury subpoenas are limited. Namely, like criminal search warrants, their purpose must have a criminal nexus.

Other subpoena authorities include those issued during the discovery or trial phases of a criminal prosecution and those issued by federal agencies pursuant to specific statutes.[41] Although they are analogous to authorities relied upon to acquire third party documents in national security or foreign intelligence gathering investigations, agency administrative subpoenas and grand jury subpoenas are unlikely to provide an alternative means to acquire third party documents in a national security investigation and thus have not been a significant issue in post 9/11 legislation.[42]

[39] Fed. R. Crim. Pro. 41(c). *See also* 18 U.S.C. § 3103a (adding to the grounds provided in Rule 41 that "a warrant may be issued to search for or seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States," and permitting delayed notice of a search in some circumstances). In general, statutes in Title 18 of the U.S. Code governing searches and seizures in criminal cases incorporate relevant sections of Federal Rule of Criminal Procedure 41 by reference. *See, e.g.*, 18 U.S.C. § 3103 (incorporating the grounds for which a search warrant may be issued). However, some provisions add statutory requirements. *See, e.g.*, 18 U.S.C. § 3109 (adding procedures for breaking doors or windows to execute a search warrant).

[40] United States v. Williams, 504 U.S. 36, 48 (1992).

[41] For example, administrative subpoenas are available for use in the investigation by the Drug Enforcement Administration; by federal agency inspectors general; and in health care fraud, child abuse, and presidential protection investigations. *See* 21 U.S.C. § 876; 5 U.S.C. App. (III) § 6; 18 U.S.C. § 3486.

[42] Subpoena authorities are unlikely to substitute for authorities applicable in national security investigations. For administrative subpoenas, one reason is that relevant statutes do not impose a gag order component; thus, national security information might be compromised. More importantly, national security investigations and the type of investigations in which such subpoenas may be used will only rarely coincide. However, criminal investigations in which grand jury subpoenas are sought may intersect with foreign intelligence investigations under FISA in situations involving criminal conduct that also has national security implications, such as international terrorism or espionage.

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act (ECPA) provides three sets of general prohibitions accompanied by law enforcement exceptions that operate under judicial supervision.[43] These address (1) the interception of wire, oral or electronic communications (wiretapping);[44] (2) access to the content of stored electronic communications and to communications transaction records;[45] and (3) the use of trap and trace devices and pen registers (essentially in and out secret "caller id" devices).[46]

ECPA generally prohibits interception of wire, oral, or electronic communications by means of an electronic, mechanical or other device but sets forth a number of exceptions to the general prohibition.[47] It limits the types of criminal cases in which electronic surveillance may be used and requires court orders authorizing electronic surveillance to be supported by 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.[48] It also limits the use and dissemination of information intercepted.[49] In addition, when an interception order expires, authorities must notify those whose communications have been intercepted.[50] Moreover, it declares that the FISA and ECPA procedures are the exclusive means for accomplishing electronic surveillance as defined in FISA and for intercepting wire, oral, or electronic communications.[51]

Whereas provisions governing interception of communications in criminal investigations reflect a concern for Fourth Amendment requirements,[52] portions of ECPA which address stored communications and the use of pen registers and trap and trace devices are less demanding and reflect Supreme Court jurisprudence suggesting that third party business records and communications entrusted to third parties are not typically protected.[53] Government authorities may have access to communications stored with providers, and related communications records, under a search warrant, subpoena, or court order,[54] or when voluntarily surrendered by providers in emergency circumstances.[55] However, as with the interception of communications, ECPA

[43] See CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle, for a more detailed discussion of the federal laws governing wiretapping and electronic eavesdropping, along with appendices including copies of the texts of ECPA and FISA.

[44] 18 U.S.C. §§ 2510-2522.

[45] 18 U.S.C. §§ 2701-2712.

[46] 18 U.S.C. §§ 3121-3127. 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).

[47] 18 U.S.C. § 2511.

[48] 18 U.S.C. §§ 2516, 2518(3).

[49] 18 U.S.C. § 2517.

[50] 18 U.S.C. § 2518(8).

[51] 18 U.S.C. § 2511(2)(f). FISA defines electronic surveillance to include more than the interception of wire, oral, or electronic communications, 50 U.S.C. § 1801(f), but places limitations on its definition based upon the location or identity of some or all of the parties to the communications involved.

[52] Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); S. Rept. 90-1097, at 66 (1967).

[53] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976); S. Rept. 99-541, at 3 (1986).

[54] 18 U.S.C. § 2503. But communications held by electronic communications providers for less than 180 days require a warrant, 18 U.S.C. § 2703(a).

[55] 18 U.S.C. § 2702.

limits the government's use and dissemination of information and requires that targets be notified.[56]

Foreign Intelligence Surveillance Act (FISA)

FISA governs the gathering of information about foreign powers, including international terrorist organizations such as al Qaeda, and their agents.[57] Although it is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes.[58]

Although some exceptions apply,[59] government agencies typically must obtain authorization from the Foreign Intelligence Surveillance Court (FISC), a neutral judicial decision maker, when gathering foreign intelligence information pursuant to FISA. Orders issued by the FISC authorize federal officials to conduct electronic surveillance[60] or physical searches;[61] utilize pen registers and trap and trace devices;[62] access specified business records and other tangible things;[63] or target U.S. persons reasonably believed to be abroad.[64]

Although requiring a nexus to a foreign power or foreign intelligence is a common theme, different standards apply for each type of FISA order. For electronic surveillance orders, FISA currently requires that an application include, among other things, a "statement of the facts and circumstances relied upon" to justify the government's belief that a target is a foreign power or its agent.[65] It must also describe the identity, if known, or a description of the specific target of the electronic surveillance and the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.[66] When the nature and location are unknown, the FISC must direct the relevant officials to provide notice to the FISC of specific information

[56] 18 U.S.C. §§ 2517, 2518(8).

[57] *See* 50 U.S.C. § 1801(a) (definition of "foreign power").

[58] For example, it extends to the collection of information necessary for the conduct of foreign affairs. *See* 50 U.S.C. § 1801(e) (definition of "foreign intelligence information").

[59] For example, FISA provides for emergency authorization of electronic surveillance or a physical search by the Attorney General in some circumstances, while an order is sought. 50 U.S.C. §§ 1805(e) and 1824(e), respectively. It also allows physical searches to be conducted in absence of a court order for periods of up to one year where the target is a foreign nation or component of a foreign nation, a faction of a foreign nation or nations not substantially composed of U.S. persons, or an entity openly acknowledged by a foreign government or governments to be directed and controlled by such government or governments, as long as the Attorney General: (1) certifies that the physical search is directed solely at a foreign power, there is no substantial likelihood that the search will "involve the premises, information, material, or property of a United States person," and proposed minimization procedures meet specified standards; and (2) fulfills various reporting requirements regarding minimization procedures. 50 U.S.C. § 1822. *See also* 50 U.S.C. § 1802 (electronic surveillance of such foreign powers for up to 1 year without a court order).

[60] 50 U.S.C. §§ 1801-1808. FISA authorizes electronic surveillance without a FISA order in specified instances involving communications between foreign powers. 50 U.S.C. § 1802.

[61] 50 U.S.C. §§ 1822-1826.

[62] 50 U.S.C. §§ 1841-1846.

[63] 50 U.S.C. §§ 1861-1862.

[64] 50 U.S.C. §§ 1881b, 1881c. As discussed *infra*, FISA also currently includes a statutory framework for targeting non-U.S. persons abroad to acquire foreign intelligence information pursuant to a joint Attorney General/Director of National Intelligence (DNI) authorization in specified circumstances. 50 U.S.C. § 1881a.

[65] 50 U.S.C. § 1804(a)(4).

[66] 50 U.S.C. §§ 1804(a)(2); 1805(c)(1)(A) and (B).

within 10 days of the date on which surveillance begins to be directed at a new facility or place.[67] FISA also requires that less intrusive means of information gathering be used before an electronic surveillance order may be granted. Specifically, an application for an order authorizing electronic surveillance must include a certification that the information sought under the order is foreign intelligence information, and that the information may not reasonably be obtained by normal investigative techniques, together with a statement of the basis upon which such certifications rest.[68] Relatedly, an application for an electronic surveillance order must specify proposed "minimization procedures."[69]

For physical searches, the government typically must provide, among other things, "the identity, if known, or a description of the target of the search," and "a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that ... the target of the physical search is a foreign power or an agent of a foreign power."[70]

For FISA orders authorizing pen registers and trap and trace devices, although limited exceptions apply,[71] an application generally must certify that "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[72]

Finally, for orders to access records and other tangible things, FISA currently requires both "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]" and an "enumeration of minimization procedures" to be applied.[73] These provisions also include recipient non-disclosure provisions, grounds for recipients to challenge such production or non-disclosure requirements, and government reporting requirements.[74]

Many of these statutes include a requirement intended to safeguard individuals' freedom of speech and other First Amendment protections. In particular, investigations generally must not be based solely on a U.S. citizen's exercise of his or her First Amendment rights.[75]

National Security Letter Statutes

Five federal statutes require businesses—namely communications providers, financial institutions, and consumer credit entities—to produce specified records to federal officials in

[67] 50 U.S.C. § 1805(a)(3).

[68] 50 U.S.C. § 1804(a)(7)(C) and (E).

[69] *Id.* at § 1804(a)(5). Minimization procedures, examined in greater detail *infra*, are safeguards which limit the government's use of collected information.

[70] 50 U.S.C. § 1823(a).

[71] The exceptions authorize: (1) emergency authorization by the Attorney General for up to 48 hours, if specified criteria are met, while an application for a FISC order is pursued; and (2) the installation and use of pen registers and trap and trace devices for up to 15 calendar days following a congressional declaration of war). 50 U.S.C. §§ 1843, 1844.

[72] 50 U.S.C. § 1842(c).

[73] 50 U.S.C. § 1861(b)(2).

[74] 50 U.S.C. §§ 1861-1862.

[75] *See, e.g.*, 50 U.S.C. §§ 1805(a)(2)(A) (electronic surveillance), 1824(a)(2)(A) (physical searches),1842(c) (pen register or trap and trace device).

national security investigations.[76] Absent a statutory prohibition or some other specific legal impediment, federal authorities are free to request, and to receive voluntarily, access to third party business records. These national security letter (NSL) statutes are designed to carve out narrow national security exceptions to prohibitions on government information gathering in ECPA, the Right to Financial Privacy Act, and the Fair Credit Reporting Act.

Unlike with warrants in criminal investigations or orders issued under FISA, NSLs are issued directly by federal officials, without approval by any judicial body. They are analogous to orders for tangible things issued in intelligence gathering investigations pursuant to FISA because they are a demand for business records and their use is confined to national security investigations. Yet unlike FISA orders, they are not issued by a court and are available for only the records of three narrow categories of businesses. Moreover, the FBI issues tens of thousands of NSLs a year,[77] while the FISA court approves only a handful of tangible-item orders a year.[78]

Only the FBI may issue NSLs under the communications provider, financial institution, and the narrower of the two consumer credit agency statutes. Authority under the other consumer credit agency statute is available to the agencies of the intelligence community, and authority under the National Security Act extends to both intelligence and law enforcement agencies.

The information available under each of the statutes varies. The National Security Act statute reaches an extensive array of financial and consumer credit records, but only applies to federal employees and individuals who have consented to disclosure of the information.[79] The more sweeping consumer credit statute extends to any consumer information held by a consumer credit reporting agency but only when sought in connection with an investigation into international terrorism.[80] The communications provider NSL statute applies to provider transaction records concerning customers' names, addresses, length of service, and billing records sought in connection with an inquiry into international terrorism or clandestine intelligence activities.[81] The more circumspect of the consumer credit NSL statutes covers credit agency records concerning consumers' names, current and former addresses, current and former places of employment, and the identification of financial institutions in which they have or had accounts—sought in connection with an inquiry into international terrorism and clandestine intelligence activities.[82] The financial institution NSL statute reaches customer transaction records of banks, credit unions, and a long list of other businesses that often deal in cash (pawn shops, casinos, car dealerships,

[76] The NSL statutes are: 18 U.S.C. § 2709 of ECPA; section 1114(a)(5) of the Right to Financial Privacy Act (12 U.S.C. § 3414(a)(5)); sections 626 and 627 of the Fair Credit Reporting Act (15 U.S.C. §§1681u and 1681v); and section 802 of the National Security Act of 1947 (50 U.S.C. § 436). For a more detailed discussion of the NSL statutes and the proposals to amend them see, CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, by Charles Doyle, and CRS Report R40887, *National Security Letters: Proposed Amendments in the 111th Congress*, by Charles Doyle.

[77] According to reports by the Department of Justice Inspector General's Office, the FBI issued 39,346 NSL requests in 2003, 56,507 in 2004, 47,221 in 2005, and 49,425 in 2006. 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) at 110.

[78] The Justice Department reported that the FISA court issued 13 tangible item orders in 2008 and 17 in 2007, *Letters* dated May 14, 2009 from Ass't Att'y Gen. Ronald Weich to Vice-President Biden, Senators Reid and McConnell, Speaker Pelosi, and Congressmen Hoyer and Boehner, www.justice.gov/nsd/foia/reading_room/2008fisa-ltr.pdf.

[79] 50 U.S.C. § 436.

[80] 15 U.S.C. § 1681v.

[81] 18 U.S.C. § 2709.

[82] 15 U.S.C. § 1681u.

jewelers, etc.), again sought in connection with an inquiry into international terrorism and clandestine intelligence activities.[83]

NSL recipients may be bound by nondisclosure requirements under each of the statutes.[84] However, they may seek judicial review of any secrecy requirement imposed and of the NSL itself.[85]

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 statutes.[86] Absent congressional intervention, three of the amendments to FISA—the lone wolf, roving wiretap, and business record provisions—will expire on December 31, 2009.

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.[87] 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. Relatedly, as discussed *infra*, the USA PATRIOT Act and subsequent measures increased the scope of international terrorism-related activities which now fall within the ambit of the federal criminal code.

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.[88]

---

[83] 12 U.S.C. § 3414(a)(5).

[84] The terms "nondisclosure requirements," "secrecy requirements," and "gag orders" are used interchangeably throughout this report.

[85] 18 U.S.C. § 3511; John Doe, Inc. v. Mukasey, 549 F.3d 861 (2d Cir. 2008). *See also* discussion regarding judicial oversight, *infra*.

[86] 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.

[87] 50 U.S.C. § 1804(a)(7)(B) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(B) (physical searches).

[88] 50 U.S.C. § 1806(k)(1) (electronic surveillance); 50 U.S.C. § 1825 (physical searches).

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."[89] 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.[90]

Another important expansion followed in the wake of revelations regarding the Terrorist Surveillance Program. Two measures, discussed in greater detail *infra*,[91] 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.[92] 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.[93] 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. [94]

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.[95] Authorities had previously limited that circle to persons believed to be agents of foreign powers.

Expansion of Electronic Surveillance Authorities

The USA PATRIOT Act amended electronic surveillance authorities in ECPA and FISA. The amendments to ECPA primarily address matters other than the interception of the content of

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

[90] *But see* Letter from Assistant Attorney General Ronald Weich to Hon. Patrick J. Leahy, at 5 (Sept. 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) Set to Expire in 2009*, by Anna C. Henning and Edward C. Liu.

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

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

[93] *Id.*

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

[95] *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.

communications. However, the Act did add several terrorism-related offenses to the list of federal crimes that may serve as the basis for an interception order.[96] It also authorizes intercepting officers to share information with various federal intelligence and law enforcement officials[97] and provides explicit disciplinary provisions for intentional violations by federal employees.[98]

Moreover, section 217 created a new exception to ECPA's general prohibition on the interception of electronic communications. The exception permits law enforcement officials to intercept the communications of an intruder into someone else's computer or computer system with the consent of system's owner or operator.[99] The exception is limited to the trespasser's communications to, through, and from the invaded system.

An additional important amendment to ECPA broadened the stored communication language in an effort to treat stored voice mail in the same manner as e-mail.[100] Finally, section 220 amended ECPA to permit nationwide service of search warrants of material held by service providers,[101] and section 212 amended it to allow for emergency disclosures by service providers.[102]

Likewise, 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.[103] As amended by P.L. 109-177, this finding must be based upon specific facts provided in the application.[104] In addition, section 207 of the USA PATRIOT Act extended the duration of FISA wiretaps and extensions thereof.[105]

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.[106]

[96] P.L. 107-56, §§ 201, 202, 18 U.S.C. § 2516(1).

[97] P.L. 107-56, § 203(b), 18 U.S.C. §§ 2510(19), 2517(1).

[98] P.L. 107-56, § 223(a), 18 U.S.C. § 2520(f).

[99] P.L. 107-56, § 217, 18 U.S.C. §§ 2511(2)(i), 2510(21).

[100] P.L. 107-56, § 209, 18 U.S.C. §§ 2703, 2510(14).

[101] P.L. 107-56, § 220, 18 U.S.C. §§ 2711, 2703.

[102] P.L. 107-56, § 212, 18 U.S.C. § 2702.

[103] 50 U.S.C. § 1805(c)(2)(B).

[104] *Id.*

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

[106] 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.[107] 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.[108] 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.[109]

Expansion of Authorities for Pen Registers and Trap and Trace Devices

The USA PATRIOT Act amended both FISA and ECPA 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."[110] However, it prohibits any investigation involving a United States person that is "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[111]

Section 216 amended the ECPA to authorize courts to issue orders for the use of pen registers and trap and trace devices anywhere within the United States.[112] The statute previously limited their application to the issuing court's jurisdiction. It also authorizes the use of such devices to capture source and addressee information for computer conversations (e.g., e-mail) as well as telephone conversations.[113]

[107] 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).

[108] 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.

[109] *Id.*

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

[111] *Id.*

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

[113] 18 U.S.C. §§ 3121, 3123.

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.

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.[114] 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.[115] Now, they require a certification that the information is relevant to, or is sought for, a particular national security investigation.[116] 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.[117] 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.[118] 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."[119]

---

[114] P.L. 107-56, §§ 328(g), 505.

[115] *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 R40887, *National Security Letters: Proposed Amendments in the 111th Congress*, by Charles Doyle.

[116] *See, e.g.*, 18 U.S.C. § 2709.

[117] 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.

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

[119] *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.

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 December 31, 2009, 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.[120] As amended, the section authorizes the FISC to issue orders for access to "any tangible things." [121] Second, the section lowered the standard which must be met before the 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.]"[122]

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.[123]

The 2006 measures also called for audits of the use of section 215 authority by the Justice Department's inspector general.[124] 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.[125] 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.[126] The 2006 amendments enlarged FISA trap and trace authority so that such "combo" FISA applications are no longer necessary.[127] The FISA court approved six "pure" section 215 requests in 2004; 14 in 2005; 15 in 2006; 17 in 2007; and 18 in 2008.[128] The IG reports suggest several reasons for the sparse use. The approval process is less familiar, multi-layered, sometimes cumbersome, and time consuming.[129] Moreover, voluntary compliance, NSLs, grand jury subpoenas, or FISA trap and trace orders can often provide access

[120] 50 U.S.C. §§ 1861-1862 (2000 ed.).

[121] 50 U.S.C. § 1861(a)(1).

[122] 50 U.S.C. §§ 1861-1863.

[123] 50 U.S.C. § 1861(a).

[124] P.L. 109-177, §§ 102(b), 106A.

[125] 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*).

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

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

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

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

to the same documents more quickly.[130] Nevertheless, the Justice Department considers section 215 authority to be a valuable tool when these alternative means are not available.[131]

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.[132] In such cases, FISA responses not infrequently included irrelevant information. After the 2006 amendments, the orders authorize government access only to relevant information.[133] However, 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.[134] 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.

New Statutory Authority to Conduct "Sneak and Peek" Searches

As a general rule, the Federal Rules of Criminal Procedure require officers executing a search warrant to give notice that they have done so and to leave an inventory of the property they have seized.[135] Section 213 of the USA PATRIOT Act, as amended, permits delayed notice search warrants under some circumstances.[136] A delayed notice, or "sneak and peek," search warrant is one that authorizes law enforcement officers to secretly enter a home or business, either physically or virtually, conduct a search, take pictures or copy documents, and depart without taking any tangible evidence or leaving notice of their presence. Before section 213, the federal courts agreed that such warrants might be issued under certain exigent circumstances, but disagreed over whether an unnoticed search in the absence of sufficient exigent circumstances constituted a Fourth Amendment violation as well as a violation of the federal rules. They also disagreed as to whether notice might be delayed for longer than seven days or some similar short period of time without court approval.[137]

The law now permits a delayed notification for 30 days or more for such warrants. In addition, the period of delay may be renewed and extended for intervals of 90 days or more if there is reason to believe that immediate notification will "result in (A) endangering the life or physical safety of an individual; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation."[138]

---

[130] *Id.*

[131] *Id.* at 58.

[132] 50 U.S.C. § 1861(b) (2000 ed., Supp. I).

[133] 50 U.S.C. § 1861(b).

[134] 50 U.S.C. § 1861(b)(2).

[135] Fed. R. Crim. P. 41(f).

[136] 18 U.S.C. § 3103a(b).

[137] See United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986); United States v. Simmons, 206 F.3d 392 (4th Cir. 2000).

[138] 18 U.S.C. §§ 3103a(b), 2705(b). In other Fourth Amendment cases, the Supreme Court has identified the destruction (continued...)

In fiscal year 2008, federal courts issued 763 delayed notice warrants, most often for 90 days.[139] Drug cases accounted for 474 of the initial warrants and for 369 of the 528 extensions granted; terrorism cases accounted for three of the warrants and two of the extensions.[140] Thus, even when there is a criminal nexus, delayed notice search warrants do not appear to be a regular employed investigative tool in national security investigations.

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.[141]

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.[142] In addition, it requires the Director of the Administrative Office to submit an annual report to Congress summarizing the use of delayed notice warrants.[143]

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

---

(...continued)

of evidence, threats to individual safety, and risk of the suspect's flight as among the permissible exigent circumstances justify delayed notice. *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 936 (1995).

[139] Administrative Office of the United States Courts, *Report of the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions*, EC-2350, 155 Cong. Rec. S7555 (daily ed. July 15, 2009) at 1-2.

[140] *Id.* at 6.

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

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

[143] *Id.*

statistical information concerning the number of emergency physical search orders authorized or denied by the Attorney General.[144] Likewise, section 128 requires that the Judiciary Committees receive full reports on the use of the FISA's pen register and trap and trace authority every six months.[145]

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.[146] The requirement was likely a response to objections that e-mail 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.[147]

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*,[148] 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.[149] 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.[150]

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 a motion to modify or set aside a nondisclosure requirement.[151] Petitions, which survive a

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

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

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

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

[148] 549 F.3d 861 (2d. Cir. 2008).

[149] 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).

[150] *Mukasey*, 549 F.3d at 883.

[151] 50 U.S.C. § 1861(f).

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.[152] As in the NSL statute provision to which the Second Circuit objected,[153] the government's certification of a possible adverse impact on national security or diplomatic relations is conclusive.[154] If a petition is denied, a renewed petition may not be filed until a year later.[155]

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.[156] 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.[157] Under FISA, minimization means, roughly, procedures to curtail the interception of the communications of Americans consistent with national security needs.[158] 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.[159] As discussed *supra*, in addition to requiring minimization procedures specific to an investigation, both ECPA and FISA also place general limitations on the use of authorities and the information collected. For example, ECPA restricts the use and dissemination of information collected.[160]

Today, the national security letter statutes have no comparable provisions, although most have dissemination limits.[161] 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

[152] 50 U.S.C. § 1861(f)(2).

[153] 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").

[154] 50 U.S.C. § 1861(f)(2)(C)(ii).

[155] 50 U.S.C. § 1861(f)(2)(C)(iii).

[156] *Cf.*, 18 U.S.C. §§ 401, 402.

[157] 18 U.S.C. § 2518(5).

[158] 50 U.S.C. § 1801(h).

[159] 50 U.S.C. §§ 1806, 1825.

[160] 18 U.S.C. §§ 2517, 2518(8).

[161] 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).

letter minimization procedures.[162] A report prepared by the Justice Department's inspector general discussed efforts of the Justice Department to formulate such procedures and reservations concerning the initial proposals.[163] The inspector general has also testified that such procedures are needed and overdue, but acknowledged that the task has proven challenging.[164] 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."[165]

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.[166] 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."[167] Accordingly, it issued interim procedures, which the inspector general concluded "do not adequately address the intent and requirements of the [law] for minimization requirements."[168]

Related Matters

A few key ancillary matters are likely to be raised in the legislative debate surrounding re-authorization of the USA PATRIOT Act and related authorities. One is the increasingly murky relationship between intelligence gathering authorities and the federal criminal code. Provisions enacted in the wake of the Terrorist Surveillance Program, including retroactive immunity for communications providers and authorities regarding persons located outside the United States that are set to expire in 2012 may also be explored.

Nexus Between Intelligence Gathering and Federal Criminal Statutes

Despite some lessening of traditional divisions between criminal law enforcement and foreign intelligence gathering resulting from the USA PATRIOT Act and subsequent measures, the purpose of government activity, and the resulting statutory framework, continues to have important consequences for the scope and nature of information collection likely to be authorized.

[162] P.L. 109-177, § 119(f).

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

[164] *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).

[165] *Id.*

[166] 50 U.S.C. § 1861(g).

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

[168] *Id.* at 87.

Searches and surveillance in criminal investigations must be justified by indicia of criminal conduct.[169] In contrast, a significant purpose of an electronic surveillance or a physical search conducted pursuant to FISA must be the collection of foreign intelligence information,[170] and those activities must be supported by 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 at which the surveillance is directed or place to be searched) is owned, possessed, in transit to or from, or is being or is about to be used by the target.[171] Likewise, the use of national security letters is generally limited to investigations of international terrorism or for clandestine intelligence activities.

Thus, the presence of a criminal law enforcement rationale is significant. Federal intelligence agents may avail themselves of grand jury subpoenas and other criminal law enforcement tools when there is a nexus to a criminal offense. The existence of that nexus often depends upon the reach of federal substantive anti-terrorism law. Federal law prohibits certain violent acts of terrorism such as aircraft sabotage and the use of weapons of mass destruction.[172] It also condemns misconduct committed in anticipation of violent acts of terrorism such as providing material support to terrorism organizations or accepting military training from terrorist organizations.[173] Moreover, terrorist offenses often serve as an element of other federal crimes such as racketeering or supply the basis for expanded procedural options in areas such as the statute of limitations.[174] For example, federal law extends the general five-year statute of limitations for prosecution of a federal crime to eight years when the offense is one defined as a federal crime of terrorism.[175]

Two federal statutes, both amended by the USA PATRIOT Act, outlaw providing material support for terrorists. One prohibits providing support for federal crimes of terrorism or similar offenses;[176] the other providing support for designated terrorist organizations.[177] The second declares in part that "[w]hoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both."[178] Conviction requires proof that the defendant either knew that the organization had been designated a foreign terrorist organization or that it engaged in terrorism.[179] It does not require the government to prove that the support was provided

[169] *See* Fed. R. Crim. P. 41(c); 18 U.S.C. § 2518(3).

[170] *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.

[171] 50 U.S.C. § 1805(a)(2)(A) and (B) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search). 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).

[172] 18 U.S.C. § 32 (destruction aircraft or aircraft facilities); 18 U.S.C. § 2332a (use of weapons of mass destruction)

[173] 18 U.S.C. § 2339B (providing material support); 18 U.S.C. § 2339D (military training). While section 2339B covers attempted violations, section 2339D does not.

[174] 18 U.S.C. §§ 1961-1962 (racketeering); 18 U.S.C. § 3286 (statute of limitations).

[175] 18 U.S.C. § 2332b(g)(5) classifies over forty federal offenses as "federal crimes of terrorism."

[176] 18 U.S.C. § 2339A.

[177] 18 U.S.C. § 2339B. Neither section explicitly covers material support of the families of terrorist suicide bombers.

[178] 18 U.S.C. § 2339B(a)(1).

[179] More precisely, it requires that it had been designated or that the organization has or is engaged in terrorist activity as defined in 8 U.S.C. § 1182(a)(3)(B), or in terrorism as defined in 22 U.S.C. § 2656f(d)(2).

with the intent to further the organization's illicit activities.[180] The Ninth Circuit has held that the terms "training" and "service" as used in these sections to describe prohibited forms of material support are unconstitutionally vague.[181] The Supreme Court has agreed to hear arguments which assert that they are incompatible with the prohibitions of the First Amendment and unconstitutionally vague.[182]

In addition to the racketeering and statute of limitation provisions, federal crimes of terrorism appear in a number of federal statutes. In some instances, the presence of a federal crime of terrorism is an element of the offense.[183] In others, investigation of a federal crime of terrorism constitutes an exception to an otherwise applicable privacy restriction.[184] As a general rule, the Sentencing Guidelines recommend more severe sentences for federal crimes of terrorism.[185]

In addition to the material support crime, federal law uses an alternative terrorism cross reference with at least equal regularity. Namely, 18 U.S.C. § 2331 provides an element for some offenses, such as one which makes it a federal crime to commit bribery affecting port security with the intent to commit international or domestic terrorism.[186] It too supplies the grounds for an exception to otherwise binding privacy restrictions.[187] And, several federal crimes are more severely punished when they are committed in furtherance of international or domestic terrorism.[188]

The difference between the two cross references is one of specificity on one hand and a terrorism nexus on the other. 18 U.S.C. § 2332b(g)(5)(B) provides a relatively limited list of specific federal crimes that need not necessarily be committed in a terrorist context.[189] 18 U.S.C. § 2331, on the other hand, includes any federal, state, or foreign crime of violence, but only if committed for terrorist purposes.[190] The domestic terrorism definition of section 2331 originated in the USA PATRIOT Act.[191] Critics have suggested that its want of specificity threatens possible misuse against political dissents.[192]

---

[180] Humanitarian Law Project v. Mukasey, 552 F.3d 916, 927 (9th Cir. 2009), *cert. granted*, ____ S.Ct. ____ (Sept. 30, 2009); United States v. Warsame, 537 F.3d 1005, 1021-22 (D. Minn. 2008).

[181] Humanitarian Law Project v. Mukasey, 552 F.3d 916, 928-30 (9th Cir. 2009), *cert. granted*, ____ S.Ct. ____ (Sept. 30, 2009).

[182] Humanitarian Law Project v. Holder (Doc. No. 08-1498), ____ S.Ct. ____ (Sept. 30, 2009); Holder v. Humanitarian Law Project (Doc. No. 09-89), ____ S.Ct. ____ (Sept. 30, 2009).

[183] 18 U.S.C. § 2283 (transportation of explosives or weapons of mass destruction knowing they are intended to be used commit a federal crime of terrorism) and § 2284 (transportation of a terrorist who intends to commit, or is in flight following commission of, a federal crime of terrorism).

[184] 20 U.S.C. §§ 1232g(j), 9573(e) (court orders for access to confidential educational records).

[185] U.S.S.G. § 3A1.4.

[186] 18 U.S.C. § 226.

[187] 20 U.S.C. § 1232g(j), § 9573(e) (court orders for access to confidential educational records).

[188] *E.g.*, 18 U.S.C. § 1001 (false statements), § 1028 (fraud relating to identification documents), § 1505 (obstruction of administrative proceedings).

[189] 18 U.S.C. § 2332b(g)(5) consists of two elements: a terrorism element ("an offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct," 18 U.S.C. § 2332b(g)(5)(A)) and one listing specific federal crimes ("an offense that . . . is a violation of [specified sections]," 18 U.S.C. § 2332b(g)(5)(B)). Most statutes cross reference only to section 2332b(g)(5)(B).

[190] *See* 18 U.S.C. § 2331(1) (defining "international terrorism"); 18 U.S.C. § 2331(5) (defining "domestic terrorism").

[191] P.L. 107-56, § 802.

[192] *See e.g.*, *How the USA PATRIOT Act Will permit Governmental Infringement upon the Privacy of Americans in the* (continued...)

Aftermath of the Terrorist Surveillance Program (TSP)

In late 2005, the *New York Times* reported that the federal government had "monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people in the United States without warrants."[193] Subsequently, President Bush acknowledged that, after the attacks of September 11, 2001, he had authorized the National Security Agency to "intercept international communications into and out of the United States" by "persons linked to al Qaeda or related terrorist organizations" based upon "his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy,"[194] despite the general rule that electronic surveillance by the federal government is unlawful unless conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) or Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[195] Now discontinued, the TSP appears to have been active from shortly after September 11, 2001, to some time in January of 2007.[196]

Following these revelations, Congress enacted the Protect America Act, P.L. 110-55, and the FISA Amendments Act of 2008, P.L. 110-261. They addressed several issues raised in public discussions regarding the TSP. Two provisions likely to arise in the current legislative debate include (1) retroactive immunity for telecommunications providers who played a role in the TSP; and (2) temporary provisions applying different procedures and standards to targets under FISA depending upon the person's nationality and geographic location.

Retroactive Immunity for Telecommunications Providers

After private citizens and interest groups became aware of the TSP, they filed dozens of lawsuits alleging various statutory and constitutional violations by the telecommunications companies that participated in the program.[197] During litigation, the government moved for the dismissal of the cases on the basis of the state secrets privilege, which bars the disclosure during litigation of information that, "in the interest of national security, should not be divulged."[198] While the district court left open the possibility that the privilege might lead to dismissal at a later date, it declined to dismiss the suits before the discovery stage in the litigation.[199]

(...continued)

Name of "Intelligence" Investigations, 150 U. Pa. L. Rev. 1651, 1688-692 (2002).

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

[194] U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, at 5, 17, Jan. 19, 2006, http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf. *See also* CRS Report R40888, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, by Elizabeth B. Bazan and Jennifer K. Elsea.

[195] The "procedures in [Title III of the Omnibus Crime Control and Safe Streets Act] and the Foreign Intelligence Surveillance Act of 1978 shall be *the exclusive means* by which electronic surveillance, as defined in section 101 of FISA, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

[196] S.Rept. 110-209, at 4. *See also* Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (January 17, 2007).

[197] *Id.* at 7.

[198] United States v. Reynolds, 345 U.S. 1, 10 (1953).

[199] Hepting v. AT&T, 439 F. Supp. 2d 974, 994 (N.D. Cal. 2006).

Insofar as many of the details of the TSP remain classified, it is likely that assertions of the state secrets privilege would have been central to the disposition of the civil suits against telecommunications providers. However, the enactment of the 2008 FISA Amendments Act provided the Attorney General with the authority to seek the dismissal of these lawsuits.[200] Under the 2008 law, no civil case against a covered telecommunications company could proceed if the Attorney General certified that any assistance given by the defendant was given in connection with the TSP between September 11, 2001, and January 17, 2007, and the defendant received written assurances that the TSP was authorized by the President and determined to be lawful.[201] Dismissal was required if the court found that the certified facts were supported by "substantial evidence." In September of 2008, Attorney General Mukasey made the necessary certification and moved to dismiss the civil suits against the telecommunications providers.[202] In June of 2009, the consolidated suits were dismissed after the district court found the certification to be supported by substantial evidence.[203] That decision was appealed to the Ninth Circuit, and is currently pending.

Were Congress to act subsequently to repeal the retroactive immunity provided by the FAA, the defendants might argue that such a repeal violates their due process rights[204] or the constitutionally required separation of powers.[205] However, courts have generally only upheld such claims where the party was in possession of a final, unreviewable judgment. Although, at this time, the cases have been dismissed by the district court, that dismissal has not been reduced to a final, unreviewable judgment as it is currently being reviewed by the Ninth Circuit. Therefore, legislative modification of the retroactive immunity enjoyed by these defendants under the FISA Amendments Act remains a possibility.

Provisions Expiring in 2012

After the TSP activities were concluded in 2007, Congress enacted the Protect America Act, which established a mechanism for the acquisition, via a certification by the Director of National Intelligence (DNI) and the Attorney General but without a court order, of foreign intelligence information concerning a person reasonably believed to be outside the United States.[206] This temporary authority ultimately expired after approximately six months, on February 16, 2008. Several months later, the Congress enacted the FISA Amendments Act of 2008, which created separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States under a new Title VII of FISA.[207] Title VII is set to expire on December 31, 2012.

[200] 50 U.S.C. § 1885a.

[201] Alternatively, the Attorney General can certify that the alleged assistance was not in fact provided by the defendant. 50 U.S.C. § 1885a(a)(5).

[202] *See* Public Certification of the Attorney General of the U.S., In re Nat'l Security Telecommunications Records Litigation, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sep. 19, 2008) (on file with author).

[203] In re NSA Telcoms. Records Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2009).

[204] Chase Sec. Corp. v. Donaldson, 325 U.S. 304, 315-316 (1945) (noting in dicta that "some rules of law probably could not be changed retroactively without hardship and oppression" to the extent that it would be considered a violation of the Due Process Clause).

[205] See Plaut v. Spendthrift Farm, Inc., 514 U.S. 211 (1995) (federal law that reopened final judgment in cases where statute of limitations barred claim was a violation of the separation of powers).

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

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

Pursuant to Title VII, non-U.S. persons reasonably believed to be abroad may be targeted to acquire foreign intelligence information pursuant to a joint Attorney General/Director of National Intelligence (DNI) authorization if certain criteria are met.[208] The authority may not be used for reverse targeting—in situations where the true focus of the collection effort is a person in the United States.[209] Title VII requires a FISC order to authorize the targeting U.S. persons reasonably believed to be abroad.[210] The targeting procedures, minimization procedures, and supporting certifications by the Attorney General and the DNI, applicable to the targeting of non-U.S. persons reasonably believed to be outside the United States, are subject to judicial review by the FISC. In addition, electronic communications service providers directed by the Attorney General and the DNI to provide assistance in connection with such acquisitions from targeted non-U.S. persons may challenge such directives before the FISC, with appeal to the Foreign Intelligence Surveillance Court of Review, and, if necessary, to the Supreme Court. Probable cause determinations, minimization procedures, and certifications with respect to the targeting of U.S. persons reasonably believed to be outside the United States are also subject to judicial review.

Conclusion

Pending legislative proposals would extend some or all of the three expiring amendments to FISA.[211] However, as with previous USA PATRIOT Act re-authorization measures, the legislative debate incorporates not just the expiring provisions but examines more broadly existing authorities for government collection of private information.

Arguments raised 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.[212] 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]."[213]

Countervailing arguments assert that amendments enacted following the 9/11 terrorist attacks undermined citizens' civil liberties unnecessarily.[214] 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

[208] 50 U.S.C. § 1881a.

[209] 50 U.S.C. § 1881a(b)(2).

[210] 50 U.S.C. §§ 1881b and 1881c.

[211] *See, e.g.*, USA PATRIOT Act Sunset Extension Act of 2009, S. 1692, 111th Cong. (2009) (proposing a four-year extension); Safe and Secure America Act of 2009, H.R. 1467, 111th Cong. (2009) (proposing a ten-year extension); Judicious Use of Surveillance Tools In Counterterrorism Efforts Act of 2009, S. 1686, 111th Cong. (2009) (proposing a permanent extension).

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

[213] *Id.*

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

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 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."[215]

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

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

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

Elizabeth B. Bazan
Legislative Attorney
ebazan@crs.loc.gov, 7-7202

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

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