NSA Surveillance Leaks: Background and Issues for Congress

John W. Rollins
Specialist in Terrorism and National Security

Edward C. Liu
Legislative Attorney

September 4, 2013

Congressional Research Service
7-5700
www.crs.gov
R43134

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Recent attention concerning National Security Agency (NSA) surveillance pertains to unauthorized disclosures of two different intelligence collection programs. Since these programs were publicly disclosed over the course of two days in June, there has been confusion about what information is being collected and under which authorities the NSA is acting. This report clarifies the differences between the two programs and identifies potential issues that may help Members of Congress assess legislative proposals pertaining to NSA surveillance authorities.

The first program collects in bulk the phone records—including the number that was dialed from, the number that was dialed to, and the date and duration of the call—of customers of Verizon and possibly other U.S. telephone service providers. It does not collect the content of the calls or the identity of callers. The data are collected pursuant to Section 215 of the USA PATRIOT ACT, which amended the Foreign Intelligence Surveillance Act (FISA) of 1978. Section 215 allows the FBI, in this case on behalf of the NSA, to apply to the Foreign Intelligence Surveillance Court (FISC) for an order compelling a person to produce "any tangible thing," such as records held by a telecommunications provider, if the tangible things sought are "relevant to an authorized investigation." Some commentators have expressed skepticism regarding how such a broad amount of data could be said to be "relevant to an authorized investigation," as required by the statute. In response to these concerns, the Obama Administration subsequently declassified portions of a FISC order authorizing this program and a "whitepaper" describing the Administration's legal reasoning.

The second program targets the electronic communications, including content, of foreign targets overseas whose communications flow through American networks. These data are collected pursuant to Section 702 of FISA, which was added by the FISA Amendments Act of 2008. This program acquires information from Internet service providers, as well as through what NSA terms "upstream" collection that appears to acquire Internet traffic while it is in transit from one location to another. Although this program targets the communications of foreigners who are abroad, the Administration has acknowledged that technical limitations in the "upstream" collection result in the collection of some communications that are unrelated to the target or that may take place between persons in the United States. Notwithstanding these technical limitations, the FISC has held that this program is consistent with the requirements of both Section 702 and the Fourth Amendment provided that there are sufficient safeguards in place to identify and limit the retention, use, or dissemination of such unrelated or wholly domestic communications.

The Obama Administration has argued that these surveillance activities, in addition to being subject to oversight by all three branches of government, are important to national security and have helped disrupt terror plots. These arguments have not always distinguished between the two programs, and some critics, while acknowledging the value of information collected using Section 702 authorities, are skeptical of the value of the phone records held in bulk at NSA. Thus, recent legislative proposals have primarily focused on modifying Section 215 to preclude the breadth of phone records collection currently taking place. They have also emphasized requiring greater public disclosure of FISC opinions, including the opinion(s) allowing for the collection of phone records in bulk.

This report discusses the specifics of these two NSA collection programs. It does not address other questions that have been raised in the aftermath of these leaks, such as the potential harm to national security caused by the leaks or the intelligence community's reliance on contractors.

Contents

Tables

Contacts

Introduction

Recent media stories about National Security Agency (NSA) surveillance address unauthorized disclosures of two different intelligence collection programs. These programs arise from provisions of the Foreign Intelligence Surveillance Act (FISA). However, they rely on separate authorities, collect different types of information, and raise different policy questions. As such, where possible, the information contained in this report distinguishes between the two. For both programs, there is a tension between the speed and convenience with which the government can access data of possible intelligence value and the mechanisms intended to safeguard civil liberties. The first program collects and stores in bulk domestic phone records that some argue could be gathered to equal effect through more focused records requests. The second program targets the electronic communications of non-U.S. persons[1] while they are abroad, but also collects some communications unrelated to those targets.

The following sections address (1) what information is being collected; (2) the legal basis for the collection; (3) existing oversight mechanisms; and (4) arguments for and against the two programs. The last section of this report discusses legislation that has been proposed in response to information disclosed about NSA surveillance. Because documents leaked to the news media may be classified, CRS is precluded from providing a detailed analysis of the content of those documents. The information in this report is based largely on public comments from intelligence officials and Members of Congress.

What Information Is Being Collected?

Domestic Collection of Domestic Phone Records—collected under Section 215 of the USA PATRIOT ACT: On Wednesday, June 5, 2013, *The Guardian* reported that NSA collects in bulk the telephone records of millions of U.S. customers of Verizon, pursuant to an order from the Foreign Intelligence Surveillance Court (FISC).[2] Intelligence officials and leaders of the congressional intelligence committees have confirmed the existence of this domestic phone records collection program, although they have not identified the companies providing the records. It has been alleged, but not confirmed, that similar orders have been sent to other telecommunications providers.[3] The court order disclosed by *The Guardian* was a three-month extension of a program that has been going on for seven years.[4] The Director of National Intelligence (DNI) has acknowledged the breadth of the program, analogizing it to "a huge library

[1] U.S. persons are defined in FISA to include U.S. citizens and legal permanent residents, as well as unincorporated associations comprised of a substantial number of U.S. persons and most domestically chartered corporations. 50 U.S.C. §1801(i).

[2] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013.

[3] Siobhan Gorman, Even Perez, Janet Hook, "U.S. Collects Vast Data Trove," The Wall Street Journal, June 7, 2013, available at http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html.

[4] Ed O'Keefe, "Transcript: Diane Feinstein, Saxby Chambliss explain, defend NSA phone records program," The Washington Post, June 6, 2013, available at http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/?print=1.

with literally millions of volumes of books," but has stated that data about Americans in the possession of the United States government can only be accessed under specific circumstances.[5]

The program collects "metadata"—a term used in this context to refer to data about a phone call, but not the phone conversation itself.[6] Intelligence officials have stated that the data are limited to the number that was dialed from, the number that was dialed to, and the date and duration of the call.[7] The data do not include cell site location information. Intelligence officials have committed to alerting Members of Congress before collecting that location information, suggesting they currently have the authority to do so.[8] The data must be destroyed within five years of acquisition.[9] Information collected does not include the location of the call (beyond the area code identified in the phone number), the content of the call, or the identity of the subscriber.[10] However, some civil liberties advocates have argued that a telephone number today is essentially a unique identifier that can be easily tied to a person's identity by other means and that the distinction between a telephone number and subscriber identity is therefore insignificant.

On June 27, 2013, *The Guardian* published an article alleging that NSA previously collected the metadata for Internet-based communications (email being the prime example) for Americans inside the United States.[11] A spokesman for the DNI confirmed *The Guardian*'s account, but said this program was discontinued in 2011. Intelligence officials have stated that, pursuant to the same FISA authorities, NSA does not currently collect in bulk the metadata of these types of communications.[12] The collection of Internet metadata was based on separate FISA authorities.[13] Some have expressed concern that those authorities could again be used to collect Internet metadata in the future.[14]

[5] The Office of the Director of National Intelligence, "Director James R. Clapper interview with Andrea Mitchell, NBC News Chief Foreign Affairs Correspondent," June 8, 2013.

[6] Metadata generally refers to "data about data" and the term could be used to refer to other information about a phone call that is not currently being collected by the government. See "Understanding Metadata," National Information Standards Organization, 2004, available at http://www.niso.org/publications/press/UnderstandingMetadata.pdf.

[7] U.S. Congress, House Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries*, 113th Congress, 1st sess., June 18, 2013.

[8] James Clapper, the Office of the Director of National Intelligence, letter to Senator Ron Wyden, July 26, 2013, available at http://www.wyden.senate.gov/news/press-releases/wyden-and-udall-important-surveillance-questions-unanswered

[9] *Id*.

[10] "Feinstein, Chambliss Statement on NSA Phone Records Program."

[11] Glenn Greenwald, Spencer Ackerman, "NSA collected US email records in bulk for more than two years under Obama," *The Guardian*, June 27, 2013, available at http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama.

[12] House Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries*.

[13] Office of the Assistant Attorney General, Department of Justice, "Report on the National Security Agency's Bulk Collection Programs Affect by USA PATRIOT Act Reauthorization," December 14, 2009, p. 3, available at http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf.

[14] See for example, Representative Nadler's comments in the House Judiciary Committee hearing on FBI oversight, June 13, 2013. "But let me ask you the following: Under Section 215 -- and I -- I would like to associate myself with the remarks that a dragnet subpoena for every - every telephone record, et cetera, every e-mail record, although I know they don't do that anymore, but they could again tomorrow, and they did do it certainly makes a mockery of the relevance of the standard in Section 215. If everything in the world is relevant, then there's no meaning to that word."

Domestic Collection of Foreign Internet-Related Data—collected under Section 702 of FISA: *The Washington Post* reported on June 6th, 2013, that, "The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[15] *The Guardian* ran a similar story that same day.[16] These articles referred to a system called PRISM allegedly used to collect this data. Outside commentators and government officials have argued that portions of these stories are inaccurate.[17] Public comments from the Administration indicate this intelligence collection is more targeted in scope than was suggested by these articles, and major technology companies have denied giving the federal government direct access to their servers.

The DNI on June 8, 2013, released a public statement saying, "*The Guardian* and *Washington Post* articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act."[18] A fact sheet provided by the DNI stated that PRISM is an internal government computer system used to facilitate access to these communications.[19] In accordance with Section 702, this collection program appears largely to involve the collection of data, including the content of communications, of foreign targets overseas whose emails and other forms of electronic communication flow through networks in the United States.[20]

Compared to the breadth of phone records collection under Section 215, this program is more discriminating in terms of its targets—it is focused on the communications of non-U.S. persons located outside the United States—but broader in terms of the type of information collected. Examples cited by the Administration include the email content of communications with individuals inside the United States, but in those cases the targets of the intelligence collection appear to have been non-U.S. citizens located outside the United States.[21]

The original press articles and more recent stories have suggested NSA monitors or can monitor the vast majority of the world's Internet traffic. NSA has stated that it "touches" only 1.6% of Internet traffic and "selects for review" 0.025% of Internet traffic. These portrayals by both critics and proponents may provide an incomplete account of NSA collection because they incorporate certain assumptions about that collection and about what types of Internet traffic are relevant to the public debate about Section 702 authorities. In August, the Office of the DNI released an October 2011 opinion of the Foreign Intelligence Surveillance Court (FISC) that provided additional insight into the scope and nature of Section 702 collection.

---

[15] Barton Gellman, Laura Poitra, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, June 6, 2013, available at http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers.

[16] Glenn Greenwald, Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian*, June 6, 2013, available at http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[17] See for example, Declan McCullagh, "No evidence of NSA's 'direct access' to tech companies," *CNET*, June 7, 2013, available at http://news.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nsas-direct-access-to-tech-companies/.

[18] The Office of the Director of National Intelligence, "DNI Statement on Activities Authorized Under Section 702 of FISA," press release, June 6, 2013.

[19] The Office of the Director of National Intelligence, "DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," press release, June 8, 2013.

[20] The President's remarks about the intelligence collection pursuant to 702 referred to "the Internet and emails."

[21] Intelligence officials have stated that communications of a U.S. person that have been inadvertently collected must be promptly destroyed unless they meet specific criteria. Examples cited by the Administration involving individuals inside the United States appear to meet these criteria.

According to the 2011 opinion, NSA collected 250 million Internet communications per year using 702 authorities.[22] Of these communications, 91% were acquired "directly from Internet Service Providers." The opinion did not identify specific providers or describe the means NSA uses to "directly" acquire communications. The other 9% were acquired through what NSA calls "upstream collection," meaning acquisition while Internet traffic is in transit from one unspecified location to another.[23] NSA also has two methods for collecting information about a specific target; "to/from" communications collection, in which the target is the sender or receiver of the Internet communications; and "about" communications collection, in which the target is mentioned in the communications of non-targets.[24] "About" communications are acquired through upstream collection.[25] Because this method does not collect the communications to or from specific individuals but rather communications that mention those individuals, it implicates a potentially broader swath of communications and raises additional civil liberties concerns.

What Are the Legal Bases for the Collection?

Domestic Phone Records: Section 215 of the USA PATRIOT ACT,[26] which is the authority under which the collection of domestic phone records has been authorized,[27] broadened government access to private business records by both enlarging the scope of materials that may be sought and lowering the legal standard required to be met.[28] Specifically, Section 215 modified the business records provisions of FISA to allow the FBI to apply to the FISC for an order compelling a person to produce "any tangible thing," including records held by a telecommunications provider concerning the number and length of communications, but not the contents of those communications.[29] In 2005, the provision was further amended to require the

[22] Foreign Intelligence Surveillance Court Memorandum Opinion, Judge John Bates, October 3, 2011, at 29, available at https://www.eff.org/file/37548#page/1/mode/1up.

[23] *Id*.

[24] *Id*., at 15.

[25] *Id*., at.17.

[26] The gathering of intelligence information not concerning a U.S. person was authorized by a technical amendment to §215 passed a few months after its enactment. *See* P.L. 107-56, §215, *amended by* P.L. 107-108, §314, *codified at* 50 U.S.C. §1861. Originally subject to sunset on December 31, 2005, §215 has been reauthorized six times since it was originally enacted, and is currently set to expire on June 1, 2015. *See*, P.L. 109-160 (extension until February 3, 2006); P.L. 109-177 (extension until December 31, 2009); P.L. 111-118, §1004 (2009) (extension until February 28, 2010); P.L. 111-141 (extension until February 28, 2011); P.L. 112-3 (extension until May 27, 2011); P.L. 112-14 (extension until June 1, 2015).

[27] Director of National Intelligence James Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, June 6, 2013, available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information. *See also* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted], No. BR 13-80 (For. Intell. Surveillance Ct. Apr. 25, 2013).

[28] Prior to 2001, FISA contained a mechanism for the government to compel the production of certain business records through subpoena-like court orders, but was limited to records from only four types of businesses: (1) common carriers, (2) public accommodation facilities, (3) storage facilities, and (4) vehicle rental facilities. A court order compelling the production of these records was authorized if the FBI presented the FISC with "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. §1862 (2001).

[29] The Supreme Court, in *Smith v. Maryland*, 442 U.S. 735 (1979), has held that there is no Fourth Amendment protected reasonable expectation of privacy in records of telephone calls held in the hands of third party providers, where the content of any call is not intercepted. However, Congress has enacted a number of statutes since the *Smith* decision, such as FISA, that both permit access by the government for foreign intelligence or law enforcement purposes (continued...)

FBI to provide a statement of facts showing that there are "reasonable grounds to believe" that the tangible things sought are "relevant to an authorized investigation (other than a threat assessment)" into foreign intelligence, international terrorism, or espionage.[30]

The phrase "reasonable grounds to believe" is not defined by FISA, but has been used interchangeably with the "reasonable suspicion" standard, a less stringent standard than "probable cause."[31] Although there are not any publicly available judicial opinions interpreting this language in the context of Section 215, it may be helpful to look at appellate courts' interpretations of the Stored Communications Act (SCA), as it similarly authorizes law enforcement to access telecommunications transactional records (as well as stored electronic communications) upon a showing that "there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation."[32] Under the SCA, the collection of stored email has been held to meet that standard in the context of a "complex, large-scale mail and wire fraud operation" in which "interviews of current and former employees of the target company suggest that electronic mail is a vital communication tool that has been used to perpetuate the fraudulent conduct" and "various sources [have verified] that [the provider who had custody of the email] provides electronic communications services to certain individual(s) [under] investigation."[33] Similarly, obtaining the internet protocol (IP) address[34] and name associated with a Yahoo! account was justified when a police officer received a tip from an individual that he had received what appeared to be child pornography from that Yahoo! account.[35]

(...continued)

to information relating to telephone numbers dialed from or received by a particular telephone number, as well as duration and usage, while simultaneously imposing limitations as to how such information may be accessed and under what circumstances it may be used.

[30] 50 U.S.C. §1861(b)(2)(A). The statute also considers records presumptively relevant if they pertain to a foreign power or an agent of a foreign power; the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. In 2005, §215 was also amended to provide special protections for records which were considered particularly sensitive. Specifically, if the records sought are "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the application must be approved by one of three high-ranking FBI officers, and cannot be further delegated. Currently, the three FBI officials who are permitted to approve such an application are Director James B. Comey; Deputy Director Sean M. Joyce; and Executive Assistant Director for National Security Stephanie Douglas. *See* 50 U.S.C. §1861(a)(3) *and* FBI, *About Us: Executives*, available at http://www.fbi.gov/about-us/executives/director.

[31] *See* U.S. v. Banks, 540 U.S. 31, 36 (2003) (forced entry into premises during execution of search warrant is permissible if there are reasonable grounds to expect futility of knocking, or if circumstances support a reasonable suspicion of exigency when the officers arrive at the door). Courts have eschewed using bright line rules to determine whether "reasonable suspicion" is warranted, and have required an examination of the totality of the circumstances instead. *See* U.S. v. Hensley, 469 U.S. 221, 227 (1985) (an informant's detailed statements implicating a third party in a bank robbery were sufficient to provide the reasonable suspicion necessary to justify a law enforcement stop of that third party); U.S. v. Brignoni-Ponce, 422 U.S. 873, 881–82, (1975) (the simple fact that a vehicle's occupants appear to be of Mexican ancestry is insufficient to provide law enforcement officers with reasonable grounds to believe that those individuals are aliens); Terry v. Ohio, 392 U.S. 1 (1968) (police officer's observation of individual repeatedly walking back and forth in front of storefronts and peering inside store windows provided reasonable suspicion that individuals were armed and about to engage in criminal activity justifying stop and frisk).

[32] 18 U.S.C. §2703(d). Note that the SCA also requires that the information be "material" rather than just "relevant."

[33] U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[34] An IP address is a numerical designation for a particular computer or device on a network that is used to facilitate routing of communications to and from that computer or device.

[35] U.S. v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

"Relevancy" is also not defined by FISA, but is generally understood to be a less stringent standard than probable cause requiring only that the information sought would tend to prove or disprove a fact at issue.[36] In August 2013, the Obama Administration released a whitepaper providing a legal analysis of the bulk collection of telephony metadata under Section 215.[37] Included in this whitepaper was an examination of the term "relevancy" as used in Section 215. The whitepaper first noted previous characterizations of relevancy by the Supreme Court described relevance as encompassing "any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case."[38] The whitepaper also noted that courts have upheld requests for "entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents."[39] On the other hand, the cases cited in the whitepaper do not appear to involve document requests which are on the same scale as the NSA's collection of domestic telephone records.[40] Nevertheless, in approving the order authorizing the NSA's collection of these records, the FISC must necessarily have agreed that Section 215's relevancy requirement had been satisfied.

An "authorized investigation" must be conducted under guidelines approved by the Attorney General under Executive Order 12333 and may not be conducted of a United States person solely upon the basis of activities protected by the First Amendment.[41] The *Attorney General's Guidelines for FBI Domestic Operations* authorize three levels of investigations: assessments, preliminary investigations, and full investigations. Preliminary investigations require an "allegation or information indicative of possible criminal or national security-threatening activity" before being initiated. Similarly, full investigations require "an articulable factual basis for the investigation that reasonably indicates" the existence of some activity constituting a federal crime, a threat to national security, or foreign intelligence. In contrast, assessments do not require any factual predicate.[42] As Section 215 explicitly requires an authorized investigation "other than a threat assessment," it is likely that Section 215 orders may only be used in conjunction with preliminary or full investigations.

Following the disclosure of the FISC order compelling Verizon to produce large amounts of telephony metadata, some commentators have expressed skepticism regarding how there could be "reasonable grounds to believe" that such a broad amount of data could be said to be "relevant to an authorized investigation," as required by the statute. Although the order has been leaked to

[36] *See* Fed. R. Evid. §401 ("Evidence is relevant if ... it has any tendency to make a fact more or less probable than it would be without the evidence ..."); *and* Black's Law Dictionary (7th ed.) (defining relevant as "logically connected and tending to prove or disprove a matter in issue; having appreciable or probative value – that is, rationally tending to persuade people of the probability or possibility of some alleged fact.").

[37] Obama Administration Whitepaper, *Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT ACT*, Aug. 9, 2013, available at https://www.eff.org/document/administration-white-paper-section-215-patriot-act.

[38] Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978).

[39] Whitepaper at 10 (citing Carrillo Huettel, LLP v. SEC, 2011 WL 601369 (S.D. Cal. Feb. 11, 2011); Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC, 2007 WL 3492762 (N.D. Ga. Nov. 5, 2007); and Chen-Oster v. Goldman, Sachs & Co., 285 F.R.D. 294 (S.D.N.Y. 2012)).

[40] *E.g.* in *Carrillo Huettel*, the court upheld the subpoena notwithstanding the possibility that the database would include account information for only hundreds of customers.

[41] 50 U.S.C. §1861(a)(2).

[42] Attorney General's Guidelines for Domestic FBI Operations (Sept. 29, 2008), available at http://www.justice.gov/ag/readingroom/guidelines.pdf. *See also* CRS Report R41780, *The Federal Bureau of Investigation and Terrorism Investigations*, by Jerome P. Bjelopera.

various media outlets, other pieces of information that would significantly help inform any understanding of how the legal standard in Section 215 is being applied have not yet been disclosed. Specifically, it is not known what was included in the statement of facts that is required to be submitted as part of the application for a Section 215 order. Similarly, there have not been any widespread disclosures of the manner in which the FISC or FICR is applying the "reasonable grounds to believe" or "relevant to an investigation" standards provided in Section 215.

Foreign Internet-Related Data: Title VII, added by the FISA Amendments Act of 2008, provides additional procedures for the acquisition of foreign intelligence information regarding persons who are believed to be outside of the United States. The DNI has stated that the recently disclosed collection of foreign intelligence information from electronic communication service providers has been authorized under Section 702 of FISA, which specifically concerns acquisitions targeting non-U.S. persons who are overseas.[43]

Prior to the enactment of Section 702, and its predecessor in the Protect America Act of 2007, FISA only authorized sustained electronic surveillance or access to electronically stored communications after the issuance of a FISC order that was specific to the target. The FISC, in authorizing electronic surveillance or a physical search, must find probable cause to believe both (1) that the person targeted by the order is a foreign power or its agent, and (2) that the subject of the search (i.e., the telecommunications or place to be searched) is owned, possessed, or will be used by the target.[44]

Section 702 permits the Attorney General (AG) and the DNI to jointly authorize targeting of persons reasonably believed to be located outside the United States, but is limited to targeting non-U.S. persons. Once authorized, such acquisitions may last for periods of up to one year. Under subsection 702(b) of FISA, such an acquisition is also subject to several limitations. Specifically, an acquisition:

- May not intentionally target any person known at the time of acquisition to be located in the United States;
- May not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- May not intentionally target a U.S. person reasonably believed to be located outside the United States;
- May not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

[43] Director of National Intelligence James Clapper, *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, June 8, 2013, available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act.

[44] 50 U.S.C. §1805(a)(3) (2008) (electronic surveillance); *Id*. at §1824(a)(3) (physical searches). In contrast, federal criminal search warrants require probable cause to believe that instrumentalities, evidence, or fruits of a crime will be found in the place to be searched. *See* Fed. R. Crim. P. 41(c). Criminal warrants authorizing electronic surveillance additionally require probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are insufficient, and that the facilities that are the subject of surveillance will be used by the target. 18 U.S.C. §2518(3) (2008).

- Must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.[45]

Acquisitions under Section 702 are also geared towards electronic communications or electronically stored information. This is because the certification supporting the acquisition, discussed in the next section, requires the AG and DNI to attest that, among other things, the acquisition involves obtaining information from or with the assistance of an electronic communication service provider.[46] This would appear to encompass acquisitions using methods such as wiretaps or intercepting digital communications, but may also include accessing stored communications or other data.

Central components of Section 702 are the targeting and minimization procedures that must be submitted to the FISC for approval. In order to be approved, Section 702 requires the targeting procedures be reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[47]

The Fourth Amendment to the U.S. Constitution protects against "unreasonable searches and seizures."[48] In domestic criminal law investigations, it generally requires law enforcement officers to obtain a court-issued warrant before conducting a search.[49] When the warrant requirement does not apply, government activity is generally subject to a "reasonableness" test under the Fourth Amendment.[50] The extent to which the warrant requirement applies to the government's collection of foreign intelligence is unclear. In a 1972 case, the Supreme Court invalidated warrantless electronic surveillance of *domestic* organizations on Fourth Amendment grounds, despite the government's assertion of a national security rationale.[51] However, it indicated that its conclusion might be different in a future case involving the electronic surveillance of foreign powers or their agents, within or outside the United States.[52]

In August 2013, the Obama Administration partially declassified several opinions of the FISC regarding collection activities under Section 702.[53] The first of these opinions, dated October 3,

[45] 50 U.S.C. §1881a(b).

[46] 50 U.S.C. §1881a(g)(2)(A)(vi).

[47] The certification must also attest that guidelines have been adopted to ensure that the specifically prohibited types of surveillance activities listed in §702(b), such as reverse targeting, are not conducted.

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

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

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

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

[52] *Id*. at 321-22. *See also* In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (U.S. Foreign Intell. Surveillance Ct. Rev. 2008) (holding that the foreign intelligence surveillance of targets reasonably believed to be outside of the U.S. qualifies for the "special needs" exception to the warrant requirement).

[53] *See* Office of the DNI, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, Aug. 21, 2013, available at
(continued...)

2011, dealt with the FISC's evaluation of the targeting and minimization procedures proposed by the government to deal with new information regarding the scope of upstream collection. Specifically, the government had recently discovered that its upstream collection activities had acquired unrelated international communications as well as wholly domestic communications due to technological limitations. After being presented with this new information, the FISC found the proposed minimization procedures to be deficient on statutory[54] and constitutional[55] grounds. With respect to the statutory requirements, the FISC noted that the government's proposed minimization procedures were focused "almost exclusively" on information that an analyst wished to use. Consequently, communications that were known to be unrelated to a target, including those that were potentially wholly domestic,[56] could be retained for up to five years so long as the government was not seeking to use that information. The court found that this had the effect of maximizing the retention of such information, and was not consistent with FISA's mandate to minimize the retention of U.S. person information.[57]

The FISC also held that the proposed minimization procedures did not satisfy the Fourth Amendment. In 2008, the Foreign Intelligence Surveillance Court of Review (FISCR) upheld collection activities under the Protect America Act (PAA)[58] that appear to have closely resembled the authority under Section 702.[59] The FISCR first determined that the purposes of foreign intelligence investigations were sufficiently important and different from traditional law enforcement to justify an exception to the warrant requirement. The court went on to hold that surveillance under the PAA was also reasonable since the targeting and minimization procedures used by the government provided sufficient proxies for the traditional particularity and probable cause requirements of the Fourth Amendment. The court especially noted that such procedures were reasonable especially when balanced against the government's interest in protecting national security, which was "of the highest order of magnitude."[60] In contrast, in the October 2011 opinion, the FISC applied the same analysis, but after having first determined that the minimization procedures were statutorily deficient, found that the balance required under the Fourth Amendment's reasonableness test did not favor the government.

A second opinion declassified by the DNI in August 2013 dealt with the aftermath of the October 2011 opinion. Under Section 702, if the FISC disapproves of the proposed minimization procedures, the government may revise those procedures in order to come into compliance.[61] In

(...continued)

http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

[54] Foreign Intelligence Surveillance Court Memorandum Opinion, at 59-63, 67-80 (Oct. 3, 2011).

[55] *Id*, at 67-79 (Oct. 3, 2011). The FISC upheld the targeting provisions, even though the government acknowledged that its upstream collection activities were known to acquire some wholly domestic communications. The FISC found that this was not a violation of Section 702, since the government could not determine "at the time of acquisition" whether a particular communication was wholly domestic. Foreign Intelligence Surveillance Court Memorandum Opinion, at 46-47 (Oct. 3, 2011).

[56] If a communication is recognized as being wholly domestic, it would have been purged from the system under the proposed minimization procedures.

[57] *Id.* at 59.

[58] P.L. 110-55. The Protect America Act expired after approximately six months, on February 16, 2008.

[59] In re Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009-1016 (U.S. Foreign Intell. Surveil Ct. Rev. 2008) (upholding similar joint authorization procedure under the Protect America Act in the face of a Fourth Amendment challenge brought by telecommunications provider).

[60] *Id.* at 1012.

[61] 50 U.S.C. §1881a(i)(3)(B).

this case, the government presented revised minimization procedures to the FISC, and the court approved those procedures on November 30, 2011.[62] The revised minimization procedures required the segregation of those communications most likely to involve unrelated or wholly domestic communications; required special handling and markings for those communications which were not segregated to warn analysts; and reduced the retention period from five years to two.[63]

What Oversight Mechanisms Are in Place?

The following is a summary of the oversight mechanisms governing the two intelligence collection programs. Both programs appear to be subject to frequent examination by the FISC, in addition to Congress. However, critics, citing the frequency with which requests are approved by the FISC, argue that the court operates as a "rubber stamp" for the executive branch.[64] Others contend that the FISC is composed of experienced judges and a professional staff and that the frequency of requests approved by the court reflects an iterative, aggressive oversight process. Because of the lack of clarity into the court's decisions, it is difficult to judge the validity of these claims.

Domestic Phone Records: The collection of phone records in bulk is conducted pursuant to FICA orders that, according to intelligence officials, must be renewed every 90 days.[65] The data are then stored at a repository at NSA. The FISC also approves the procedures governing access to those data and has apparently required that NSA meet a *reasonable articulable suspicion standard* prior to searching the data.[66] FISC approval is not necessary prior to searching the data already held at NSA. Rather, 22 individuals at NSA have been authorized to approve requests to query the data and to determine whether information meets the reasonable suspicion standard.[67]

Queries against phone records data are documented and audited by NSA. In 2012, less than 300 phone numbers were used to query the database.[68] Intelligence officials have identified several additional oversight mechanisms that monitor the implementation of this program. These include (1) a report filed every 30 days with the FISC; (2) a meeting at least every 90 days between the Department of Justice (DOJ), the Office of the Director of National Intelligence (ODNI), and NSA, and (3) a semiannual report to Congress.

---

[62] Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (Nov. 30, 2011).

[63] *Id.* at 7-11. A third and final declassified order was issued in September of 2012 and addressed the question of what to do with the information that had been acquired through upstream collection prior to the October 2011 opinion. In this third opinion, the FISC acknowledged that the NSA had made a "corporate decision" to purge all data identified as originating from upstream collection before October 31, 2011 (the date that the revised minimization procedures went into effect). Foreign Intelligence Surveillance Court Memorandum Opinion, at 11-15 (Sept. 2012).

[64] For example, from 2010 to 2012, the court granted all but one of the government's 5,180 requests. See "Foreign Intelligence Surveillance Act Court Orders 1979-2011," The Electronic Privacy Information Center, available at http://epic.org/privacy/wiretap/stats/fisa_stats.html

[65] House Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries.*

[66] For a discussion of the "reasonable articulable suspicion" standard, s*ee supra* note 19 and accompanying text.

[67] House Permanent Select Committee on Intelligence, How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries.

[68] *Id*.

Foreign Internet-Related Data: The collection of electronic communications pursuant to Section 702 is subject to a less stringent oversight regime. "[I]nformation is obtained with the FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence."[69] In accordance with the FISA Amendments Act, procedures governing the program, designed to prevent the acquisition and dissemination of Americans' communications, are subject to court approval.[70] Actual collection of this information does not require a warrant or court order. Decisions regarding whether collection on a foreign target is in keeping with Section 702 appear to take place largely within the DOJ and ODNI.

After data are collected, NSA is subject to a number of oversight reporting procedures. These include (1) quarterly reports to the FISC concerning compliance issues; (2) semi-annual reports to the FISC and Congress that assess compliance with targeting and minimization standards; (3) semi-annual reports to the FISC and Congress on the implementation of the program; and (4) annual reviews from the NSA Inspector General.

Arguments For and Against the Two Programs

The Administration has argued that the surveillance activities leaked to the press, in addition to being subject to oversight by all three branches of government, are important to national security and have helped disrupt terror plots. These arguments have not always distinguished between the two programs, but generally the Administration appears to have taken the position that collection pursuant to Section 702 is an important tool on a broad range of national security issues and that collection pursuant to Section 215 has been useful in a discrete number of terrorism cases. Regarding bulk phone records, which have come under greater scrutiny, intelligence officials have argued that the breadth of the collection is necessary to ensure all relevant information is available to the government and can be identified through searches in NSA's database, rather than having more focused collection that might miss relevant information. For example, Deputy Attorney General James Cole before the HPSCI stated "if you're looking for a needle in the haystack, you have to get the haystack first."[71]

Intelligence officials initially stated that the two programs have "helped prevent over 50 potential terrorist events"—which appear to encompass both active terror plots targeting the United States homeland and terrorism facilitation activity not tied directly to terrorist attacks at home or abroad.[72] NSA Director General Alexander subsequently clarified these remarks, citing a total of 54 terrorist events. Forty-two of these involved terrorist plots and 12 involved material support to terrorism. Of the total number of terrorist events, 53 somehow involved collection pursuant to Section 702. Thirteen of the 54 involved threats inside the United States, and 12 of those cases somehow utilized the phone records held by NSA.[73]

[69] The Office of the Director of National Intelligence, "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," press release, June 8, 2013.

[70] P.L. 110-261.

[71] House Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries.*

[72] *Id*.

[73] General Keith Alexander, "Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War," comments before the Aspen Security Forum, July 18, 2013, available at http://aspensecurityforum.org/2013-
(continued...)

Intelligence officials have provided one example in which the target of the plot was the U.S. homeland and for which the phone records were somehow utilized. Of the other 11 cases in which the phone records were used, one involved U.S.-based material support for extremist activity outside the United States.[74] It is not clear how many, if any, of the remaining 10 cases that utilized the phone records involved terror plots targeting the U.S. homeland as opposed to U.S.-based material support for terrorism. The Administration has provided four examples:

- **Najibullah Zazi**: NSA, using *702 authorities*, intercepted an email between an extremist in Pakistan and an individual in the United States. NSA provided this email to the FBI, which identified and began to surveil Colorado-based Najibulla Zazi. NSA then received Zazi's phone number from the FBI, checked it against phone records procured using *215 authorities*, and identified one of Zazi's accomplices, an individual named Adis Medunjanin. Zazi and Medunjanin were both subsequently arrested and convicted of planning to bomb the New York City subway.[75] Additional information on this case is offered in the next section.
- **Khalid Ouazzani**: NSA, using *702 authorities*, intercepted communication between an extremist in Yemen and an individual in the United States named Khalid Ouazzani. Ouazzani was later convicted of providing material support to al-Qaeda and admitted to swearing allegiance to the group. The FBI has claimed that Ouazzani was involved in the early stages of a plot to bomb the New York Stock Exchange.[76]
- **David Headley:** According to intelligence officials, the FBI received information indicating that Headley, a U.S. citizen living in Chicago, was involved in the 2008 attack in Mumbai that took the lives of 160 people. NSA, using *702 authorities*, also became aware of Headley's involvement in a plot to bomb a Danish newspaper. It is unclear from public statements how Headley first came to the FBI's attention. He pled guilty to terrorism charges and admitted to involvement in both the Mumbai attack and Danish newspaper plot.
- **Basaaly Saeed Moalin:** NSA, using phone records pursuant to *215 authorities*, provided the FBI with a phone number for an individual in San Diego who had indirect contacts with extremists overseas. The FBI identified the individual as Basally Saeed Moalin and determined that he was involved in financing extremist activity in Somalia.[77] Moalin was convicted in 2013 of providing material support to al-Shabaab, the Somalia-based al-Qaeda affiliate.[78]

(...continued)

video.

[74] *Id*.

[75] Intelligence community backgrounder on NSA surveillance, available at http://www.fas.org/sgp/news/2013/06/ic-back.pdf.

[76] Brian Ross, Aaron Katersky, James Gordon, and Lee Ferran, "NSA Claim of Thwarted NYSE Plot Contradicted by Court Documents," *ABC News*, June 19, 2013, available at http://abcnews.go.com/Blotter/nsa-claim-thwarted-nyse-plot-contradicted-court-documents/story?id=19436557.

[77] Peter Bergen, David Sterman, "What U.S. learned from listening in on terror group calls," CNN, June 19, 2013.

[78] The Federal Bureau of Investigation, "San Diego Jury Convicts Four Somali Immigrants of Providing Support to Foreign Terrorists," press release, February 22, 2013, available at http://www.fbi.gov/sandiego/press-releases/2013/san-diego-jury-convicts-four-somali-immigrants-of-providing-support-to-foreign-terrorists.

Concerns Regarding Domestic Phone Records: Criticism has increasingly focused on the collection of phone records pursuant to Section 215. The public and Members of Congress have expressed particular concern about data provided to NSA in bulk about U.S. citizens. Critics question the importance of the phone records in the cases identified by the Administration and question whether any value from those records could have been derived from a more traditional court order. Rather than using a phone number to query a database at the NSA, they argue the same number could be given to phone companies to conduct a search of their records. This could produce similar results, although the process of obtaining the order and making a request could take longer. In essence, using the government's needle-in-a-haystack analogy, critics are suggesting that the "haystack" could be utilized to equal effect regardless of whether it is sitting at the NSA or remains in the possession of the phone company. For example, Senators Ron Wyden and Tom Udall, in a statement from June 19, 2013, argued:

> [I]t is still unclear to us why agencies investigating terrorism do not simply obtain this information directly from phone companies using a regular court order. If the NSA is only reviewing those records that meet a "reasonable suspicion" standard, then there is no reason it shouldn't be able to get court orders for the records it actually needs. Making a few hundred of these requests per year would clearly not overwhelm the FISA Court. And the law already allows the government to issue emergency authorizations to get these records quickly in urgent circumstances....
>
> [W]e have yet to see any evidence that the bulk phone records collection program has provided any otherwise unobtainable intelligence. It may be more convenient for the NSA to collect this data in bulk, rather than directing specific queries to the various phone companies, but in our judgment convenience alone does not justify the collection of the personal information of huge numbers of ordinary Americans if the same or more information can be obtained using less intrusive methods.[79]

Concerns Regarding Foreign Internet-Related Data: Many critics of Section 702 collection appear to agree that it is a valuable tool for national security, but question whether the program has been implemented, or can be implemented, in a way that adequately protects American civil liberties. Some argue that for certain types of electronic communications, it is not possible to assess with enough confidence whether a prospective target is inside the United States or overseas.

This concern sharpened in August 2013, when the Office of the DNI released the October 2011 FISC opinion in which the court found that some elements of the 702 collection program were inconsistent with the Fourth Amendment of the Constitution. The problem concerned "about" communications and NSA's "upstream collection," which are described earlier in this report. Because of technical constraints, NSA was unable to specifically collect the relevant "about" communication and instead was collecting groupings of communications, which contained communications about legitimate targets as well as communications unrelated to those targets. In some cases, that involved the collection of Americans' communications and of wholly domestic communications. As a result of this overcollection, NSA acquired tens of thousands of domestic communications, which the court determined was in violation of the Constitution.

[79] "Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs," press release, June 19, 2013, available at http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs.

As discussed above, the FISC allowed the problematic upstream "about" collection to continue but required NSA to implement stricter minimization procedures for tranches of data that might contain Americans' communications. Members may wish to engage intelligence officials about the effectiveness of NSA's "about" communications collection, which does not specifically collect the communications of foreign intelligence targets and might therefore be of less utility than "to/from" communications, which comprise 91% of collection under Section 702. While "about" communications apparently present challenging technical issues, Section 702 might nonetheless be amenable to legislative fixes if the collection that raises the greatest concerns also has the least utility.

Additional Background on Najibullah Zazi

The Zazi case cited by the Administration may help Members evaluate the utility of NSA's bulk phone records collection program. A significant amount of public information about that case has been made available since Zazi's arrest on September 19, 2009. Zazi, Medunjanin, and a third man traveled to Pakistan on August 28, 2008, to receive training from al-Qaeda. Zazi returned to the United States in January 2009.[80] Medunjanin returned in September 2008. On September 6, 2009, Zazi sent an email from Colorado to an associate in Pakistan requesting a recipe for explosives. There is reason to believe this email is the one intercepted by NSA using 702 authorities and then passed to the FBI.[81] The FBI opened an investigation and began surveillance of Zazi on September 7. Zazi traveled from Denver to New York on September 9, 2009, for the purpose of conducting an attack sometime between September 14 to 16. FBI agents observed his departure from Denver. Zazi became aware of FBI surveillance while in New York and chose to return to Denver on September 12. He was interviewed and arrested by the FBI several days later.

It is unclear at what point in the investigation authorities utilized the phone records at NSA to link Zazi to Medunjanin. FBI officials recently acknowledged that they were already aware of Medunjanin, but stated that the information derived from Section 215 collection provided corroborating information regarding Medunjanin's connection to Zazi.[82] At some point in the investigation, the FBI was able to identify travel records showing that Zazi and Medunjanin in 2008 departed for Pakistan together.[83] It has also been reported that the New York Police Department had previously identified both Zazi and Medunjanin using informants and undercover officers at a mosque in Queens.[84] Prospective questions about the role of the phone records in the investigation include the following:

- What did the FBI know about Medunjanin's travel to Pakistan and about his activity more generally prior to linking him with Zazi using the phone records

[80] Transcript of Record, U.S. v. Zazi, No. 1:10-CR-60 (E.D.N.Y. July 18, 2011).

[81] Intelligence officials have stated that an email collected using 702 authorities provided the key lead in the Zazi case. Separately, FBI officials in 2011 stated that they were tipped off to Zazi's activity when they were provided with his email from September 6th, 2009, to associates in Pakistan.

[82] U.S. Congress, House Judiciary Committee, *Oversight of the Foreign Intelligence Surveillance Act Authorities,* 113th Congress, 1st sess., July 17, 2013.

[83] Transcript of Record, U.S. v. Zazi, No. 1:10-CR-60 (E.D.N.Y. July 18, 2011).

[84] Adam Goldman, Eileen Sullivan, Matt Apuzzo, "NYPD's spying programs produced mixed results," December 23, 2011, available at http://abclocal.go.com/kfsn/story?section=news/national_world&id=8477480.

database? Was that information sufficient to link him to Zazi absent a search of those phone records?

- To what extent was the information available to FBI agents in September 2009 sufficient to obtain phone records through a court order or a National Security Letter, rather than through the repository at NSA?
- Were the phone records connecting Zazi to Medunjanin from before or after their trip to Pakistan in August 2008? In light of when those calls were made, would company retention times for phone records have limited government access to data if those records had been provided pursuant to a more specific court order?
- Was the speed with which authorities were able to access phone records data important to identifying Medunjani or to disrupting the plot? Authorities appear to have had a nine-day window during which they could exploit available information to disrupt the attack. Were phone records utilized within that window?

Legislative Proposals

To date, legislative proposals have focused primarily on intelligence collection of domestic phone records. Members of Congress have introduced bills or are circulating draft bills that would limit in various ways the scope of requests for business records that could be covered under Section 215 of the USA PATRIOT ACT of 2001. Answers to the questions above concerning the Zazi case might help elucidate the policy dimensions of these proposals. The Administration has stated that it is currently looking at the architectural framework of the Section 215 collection program and will provide recommendations to Congress on how Section 215 might be changed.[85]

Prospective changes that could require the federal government to make individualized requests to phone companies, rather than requests for phone records in bulk, could also require mandating specific retention times for phone company business records such that those times are consistent with the current five-year period for records held by NSA. The crux of the debate may come down to concerns about the speed with which the government can access phone records that are not held in bulk at NSA. With respect to changes to Section 215, NSA Director General Alexander has stated, "The concern is speed in crisis."[86] The process for identifying prospective terrorists could be slowed to some degree if the government is required to make individual requests rather than having ready access to bulk phone data. One question for Members of Congress may be whether that increased time frame would have been detrimental in any of the roughly 10 cases identified by the intelligence community that involved phone records collected in bulk.

Some Members have also proposed legislation intended to provide greater transparency of opinions of the FISC and FISCR.[87] Under current law, the opinions of either court that include

[85] House Permanent Select Committee on Intelligence, *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries.*

[86] *Id*.

[87] The precise boundaries of Congress's authority to require the declassification of material classified by the executive have not been fully explored. In one of the few cases to address disputes between the legislative and executive branches over access to classified information, the D.C. Circuit rejected the argument that the executive branch exercises plenary (continued...)

significant construction or interpretation of any provision of FISA must be provided to the judiciary and intelligence committees of the House and the Senate within 45 days.[88] However, the AG and DNI may redact information from those opinions where necessary to protect the national security of the United States and when limited to sensitive sources and methods information or the identities of targets.[89] Recent legislative proposals would further require such opinions to be made public or summarized in an unclassified manner, but would continue to provide discretion for the AG to limit the disclosure of opinions or summaries if necessary to protect national security.

Of the 22 proposals identified below, 16 include changes to Section 215 and 15 of those attempt to limit the bulk collection of phone records by NSA. Eight proposals would change the FISA process by, among other things, requiring greater public disclosure of FISA court decisions or changing the way judges are appointed to the FISA court.

Table 1. Legislative Proposals in the 113th Congress

	Includes Changes to...			
Proposals	**215**	**702**	**FISC**	**Details**
S. 1182 (Udall)	√			Would amend the business records provision of FISA to require records to pertain to the subject of the investigation, or the subject's activities or acquaintances, in addition to being relevant.
S. 1168 (Sanders, Restore Our Privacy Act)	√			Would amend the business records provision to require "specific and articulable facts" demonstrating that each of the tangible things sought is relevant prior to gaining access to records. Expands reporting requirements such that the AG is required to keep Congress fully informed regarding business records requests.
S. 1130 (Merkley, Ending Secret Law Act) **H.R. 2475** (Schiff, Ending Secret Law Act) **H.R. 2440** (Jackson Lee, FISA Court in the Sunshine Act of 2013)	√	√	√	Requires the public disclosure of orders or opinions that include "significant construction or interpretation" of Sections 215 or 702.

(...continued)

and exclusive authority over access to national security information. U.S. v. AT&T, 551 F.2d 384 (D.C. Cir. 1976). However, in practice, disputes of this matter are typically resolved through voluntary, mutually agreeable accommodation by the branches, rather than resort to judicial enforcement of asserted legal rights.

[88] 50 U.S.C. §1871(c)(1). Any judge who authors an opinion, order, or other decision may request that it be published. If the presiding judge chooses to direct publication of that order, the court may have the executive review and redact it as necessary. Foreign Intel. Surveillance Ct. R. 62.

[89] 50 U.S.C. §1871(d).

Proposals	Includes Changes to... 215	702	FISC	Details
S. 1121 (Paul, Fourth Amendment Restoration Act of 2013)				Specifies that "The Fourth Amendment to the Constitution shall not be construed to allow any agency of the United States Government to search the phone records of Americans without a warrant based on probable cause."
S. 1215 (Leahy, FISA Accountability and Privacy Protection Act of 2013)	√	√	√	Would, among other things, change the date when Section 702 authorities established in the FISA Amendments Act would expire and limit the scope of requests pursuant to Section 215 in a similar manner as S. 1182.
H.R. 2399 (Conyers, The LIBERT-E Act)	√			Would amend the business records provision to require that records be both relevant and material, as well as pertaining only to the subject of the investigation. Requires the AG to make all reports to the Intelligence and Judiciary Committees available to all Members of Congress.
H.Amdt. 413 (Amash)	√			Would have limited the availability of funds for the collection of phone records in bulk.
H.Amdt. 412 (Pompeo)	√	√		Would have limited the availability of funds for the targeting of U.S. persons pursuant to Section 702 authorities and for the collection of the content of communications pursuant to Section 215 authorities.
H.R. 2818 (Holt, Surveillance State Repeal Act)	√	√	√	Repeals the USA PATRIOT ACT. Repeals the FISA Amendments Act. Extends the term limits for FISC judges.
H.R. 2586 (Cohen, FISA Court Accountability Act)			√	Changes how judges are appointed to the FISC such that 8 of 11 judges would be designated by Members of the House and Senate.
H.R. 2761 (Schiff, Presidential Appointment of FISA Court Judges Act)			√	Gives the President the power to appoint, and the Senate the power to confirm, FISC judges.
S. 1467 (Blumenthal, FISA Court Reform ACT of 2013)			√	Establishes a position of Special Advocate with the responsibility to review applications to the FISC and decisions of the court. Requires the public disclosure of FISC decisions.
S. 1460 (Blumenthal, FISA Judge Selection Reform Act)			√	Expands the number of FISC judges to 13. Changes how judges are appointed to the FISC such that judges are nominated by the chief judge of each judicial circuit and then designated by the Chief Justice of the United States.
H.R. ____ (Fitzpatrick, NSA Accountability Act of 2013)	√			Would amend the business records provision to require that records be both relevant and material, as well as pertaining only to the subject of the investigation.

Proposals	Includes Changes to... 215	702	FISC	Details
H.R. 2603 (Ross, Relevancy Act)	√			Would amend the business records provision to require the subject of the investigation to be a specific person or a specific group of persons.
H.R. 2684 (Lynch, Telephone Surveillance Accountability Act of 2013)	√			Would amend the business records provision to prohibit searching telephony metadata, unless a FISA court judge issues an order finding that there is a reasonable, articulable suspicion that the basis of the search is material and specifically relevant to an authorized investigation.
H.R. 2736 (Larsen-Amash, Government Surveillance Transparency Act of 2013)	√	√		Authorizes a private entity that receives an order or directive under FISA to publicly disclose general and aggregate information about the information sought.
H.R. 3035 (Lofgren, Surveillance Order Reporting Act of 2013)	√	√		Permits public reporting by electronic communications providers of estimate of government requests for information.
S. 1452 (Franken, Surveillance Transparency Act of 2013)	√	√		Enhances reports to Congress on number of applications made and orders granted under FISA, as well as estimates on the number of U.S. persons affected.
H.R. 2849 (Lynch, Privacy Advocate General Act of 2013)			√	Establishes an Office of the Privacy Advocate General in the executive branch appointed jointly by Chief Justice and Senior Associate Justice, who would be required to: serve as opposing counsel for FISA applications, and authorized to request disclosure of a FISC order and appeal such orders.

Source: Prepared by CRS.

Author Contact Information

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

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

Acknowledgments

Jared Cole, Law Clerk in the American Law Division of CRS, contributed to the discussion of proposed legislation in this report. This report was originally co-authored with Marshall Curtis Erwin, formerly an Analyst in Intelligence and National Security at CRS.