NSA Surveillance Leaks: Background and Issues for Congress

Marshall Curtis Erwin
Analyst in Intelligence and National Security

Edward C. Liu
Legislative Attorney

July 2, 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 what authorities the NSA is acting under. 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.

One program collects in bulk the phone records—specifically the number that was dialed from, the number that was dialed to, and the date and duration of the call—of customers of Verizon Wireless 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," including records held by a telecommunications provider concerning the number and length of communications, but not the contents of those communications. The FBI must provide a statement of facts showing that there are "reasonable grounds to believe" that the tangible things sought are "relevant to an authorized investigation." 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.

The other program collects the electronic communications, including content, of foreign targets overseas whose communications flow through American networks. The Director of National Intelligence has acknowledged that data are collected pursuant to Section 702 of FISA. As described, the program may not intentionally target any person known at the time of acquisition to be located in the United States, which is prohibited by Section 702. Beyond that, the scope of the intelligence collection, the type of information collected and companies involved, and the way in which it is collected remain unclear. Section 702 was added by the FISA Amendments Act of 2008. Prior to the enactment of Section 702, FISA only permitted sustained domestic electronic surveillance or access to domestic electronically stored communications after the issuance of a FISC order that was specific to the target.

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

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. citizens but may incidentally collect information about Americans.

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 Wireless, pursuant to an order from the Foreign Intelligence Surveillance Court (FISC).[1] 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.[2] The court order disclosed by *The Guardian* was a three-month extension of a program that has been going on for seven years.[3] The Director of National Intelligence (DNI) has acknowledged the breadth of the program, analogizing it to "a huge library 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.[4]

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

[2] 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.

[3] 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.

[4] The Office of the Director of National Intelligence, "Director James R. Clapper interview with Andrea Mitchell, NBC
(continued...)

The program collects "metadata"—a term used in this context to refer to data about a phone call but not the phone conversation itself.[5] 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.[6] The data must be destroyed within five years of acquisition.[7] 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.[8] 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.[9] 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.[10] It has been suggested that this type of collection was also conducted pursuant to the same FISA Section 215 authorities, and some have expressed concern that those authorities could again be used to collect Internet metadata in the future.[11]

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."[12] *The Guardian* ran a similar story that same day.[13] These articles referred to a system called PRISM allegedly used to collect this data. Outside

(...continued)

News Chief Foreign Affairs Correspondent," June 8, 2013.

[5] Metadata generally refers to "data about data" and the term could be used to refer 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.

[6] 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.

[7] Ibid.

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

[9] 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.

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

[11] 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."

[12] 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.

[13] 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.

commentators and government officials have argued that portions of these stories are inaccurate.[14] 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."[15] A fact sheet provided by the DNI stated that PRISM is an internal government computer system used to facilitate access to these communications.[16] 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.[17]

Compared to the breadth of phone records collection under Section 215, this program is more discriminating in terms of its targets but broader in terms of the type of information collected. Beyond that, the scope of the intelligence collection, the type of information collected and companies involved, and the way in which it is collected remain unclear. 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.[18]

On June 20, 2013, *The Guardian* also published NSA's targeting and minimization procedures for information collected under Section 702 authorities. Documents referred to in the article specify the procedures used to determine that the targets of intelligence collection are non-U.S. persons located outside the United States and the procedures used to minimize the retention and dissemination of information about U.S. persons collected under Section 702 authorities.[19]

What Are the Legal Bases for the Collection?

Domestic Phone Records: Prior to 2001, FISA contained a mechanism for the government to compel the production of certain business records through subpoena-like court orders. Under this authority, only four types of documents could be sought in foreign intelligence or international terrorism investigations, namely records from (1) common carriers, (2) public accommodation facilities, (3) storage facilities, and (4) vehicle rental facilities.[20] A court order compelling the

[14] 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/.

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

[16] 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.

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

[18] 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.

[19] Glenn Greenwald, James Ball, "The top secret rules that allow NSA to use US data without a warrant," *The Guardian*, June 20, 2013, available at http://www.guardian.co.uk/world/2013/jun/20/fisa-court-nsa-without-warrant.

[20] 50 U.S.C. §1862(a) (2001).

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."[21]

Section 215 of the USA PATRIOT ACT,[22] which is the authority cited by the DNI as the basis of the recently revealed collection of domestic phone records,[23] broadened government access by both enlarging the scope of materials that may be sought and lowering the legal standard required to be met. 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.[24] In 2005, the provision was further amended to require the 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.[25] The statute 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.[26]

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

[21] 50 U.S.C. §1862(b)(2)(B) (2001).

[22] 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).

[23] 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.

[24] 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 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.

[25] 50 U.S.C. §1861(b)(2)(A). 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 Robert S. Mueller, III; 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.

[26] 50 U.S.C. §1861(b)(2)(A).

cause."[27] 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."[28] 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."[29] Similarly, obtaining the internet protocol (IP) address[30] 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.[31]

"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.[32]

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.[33] 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

[27] *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).

[28] 18 U.S.C. §2703(d). Note that the SCA also requires that the information be "material" rather than just "relevant."

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

[30] 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.

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

[32] *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.").

[33] 50 U.S.C. §1861(a)(2).

require any factual predicate.[34] 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 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.[35]

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.[36]

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:

---

[34] 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.

[35] 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.

[36] 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).

- 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
- Must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States.[37]

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.[38] 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.[39]

The Fourth Amendment to the U.S. Constitution protects against "unreasonable searches and seizures."[40] In domestic criminal law investigations, it generally requires law enforcement officers to obtain a court-issued warrant before conducting a search.[41] When the warrant requirement does not apply, government activity is generally subject to a "reasonableness" test under the Fourth Amendment.[42] 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

[37] 50 U.S.C. §1881a(b).

[38] 50 U.S.C. §1881a(g)(2)(A)(vi).

[39] 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.

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

[41] *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.").

[42] 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).

grounds, despite the government's assertion of a national security rationale.[43] 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.[44]

There are no publicly available judicial opinions analyzing the collection activities under Section 702 under the Fourth Amendment.[45] However, in 2008, the Foreign Intelligence Surveillance Court of Review (FISCR) upheld collection activities under the Protect America Act (PAA)[46] that appear to have closely resembled the authority under Section 702.[47] 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."[48]

While the targeting and minimization procedures applicable to Section 702 surveillance have been leaked to various press outlets, the targeting and minimization procedures the FISCR reviewed, and approved, with respect to the earlier PAA remain classified. Without the ability to compare these two sets of targeting and minimization requirements, it is difficult, if not impossible, to assess whether the reported collection activities under Section 702 are consistent with the FISCR opinion upholding the PAA.

What Oversight Mechanisms Are in Place?

The following is a summary of the oversight mechanisms governing the two intelligence collection programs, based almost entirely on testimony by intelligence community officials before the House Permanent Select Committee on Intelligence (HPSCI). Both programs appear to

[43] 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).

[44] *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. Survellance 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).

[45] Upon enactment of Title VII, a number of organizations brought suit challenging the joint authorization procedure for surveillance of non-U.S. persons reasonably believed to be abroad. The suit alleged that this authority violated the Fourth Amendment's prohibition against unreasonable searches. In order to establish legal standing to challenge Title VII, the plaintiffs had argued that the financial costs they incurred in order to avoid their reasonable fear of being subject to surveillance constituted a legally cognizable injury. However, on February 26, 2013, in *Clapper v. Amnesty International*, the United States Supreme Court held that the plaintiffs had not suffered a sufficiently concrete injury to have legal standing to challenge Title VII. Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013). Because the Court had no jurisdiction to proceed to the merits of the plaintiffs' claims, it did not decide the Fourth Amendment question. Following the recent disclosures concerning the collection of information under §702, some have argued that it may be easier to demonstrate injury for standing purposes. For a more detailed discussion, *see* CRS Report R43107, *Foreign Surveillance and the Future of Standing to Sue Post-Clapper* , by Andrew Nolan.

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

[47] 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).

[48] *Id.* at 1012.

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.[49] 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 pursuant to FICA orders that, according to intelligence officials, must be renewed every 90 days.[50] 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.[51] 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.[52]

Queries against phone records data are documented and audited by NSA. In 2012, less than 300 phone numbers were used to query the database.[53] 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.

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."[54] 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.[55] 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)

---

[49] 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

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

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

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

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

[54] 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.

[55] P.L. 110-261.

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."[56]

According to intelligence officials, 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.[57] Of these, over 90% somehow involved collection pursuant to Section 702. Of the 50, at least 10 cases included homeland-based threats, and a majority of those cases somehow utilized the phone records held by NSA. 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.[58] 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.[59]

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

[57] Ibid.

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

[59] 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.

- **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.[60] Moalin was convicted in 2013 of providing material support to al-Shabaab, the Somalia-based al-Qaeda affiliate.[61]

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.[62]

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

[61] 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.

[62] "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.

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.[63] 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 the NSA using 702 authorities and then passed to the FBI.[64] 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. Prospective questions about the role of those records in the investigation include:

- 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.[65]

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

[64] 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.

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

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."[66] 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 timeframe 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.[67] Under current law, the opinions of either court that include 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.[68] 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.[69] 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.

Legislative proposals in the 113th Congress include:

- **S. 1182** (Udall): A bill to modify the Foreign Intelligence Surveillance Act of 1978; introduced June 18, 2013. This bill would amend Section 501 of FISA—the business records section amended by Section 215 of the USA PATRIOT ACT—to require specific evidence for access to those records.
- **S. 1168** (Sanders, Restore Our Privacy Act): This bill would amend Section 501 of FISA "to limit overbroad surveillance requests." It also would expand reporting requirements for requests for records under Section 501.
- **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): These bills would require the public disclosure of opinions, decisions, and orders of the FISC that include significant legal interpretations of Section 501 or 702 of

[66] Ibid.

[67] 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 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.

[68] 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.

[69] 50 U.S.C. §1871(d).

FISA. They also include provisions that would allow the Attorney General to withhold such decisions in the interest of national security.

- **S. 1121** (Paul, Fourth Amendment Restoration Act of 2013): This bill 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. ___(Leahy, The FISA Accountability and Privacy Protection Act of 2013): This bill would change the sunset for the FISA Amendments Act from December 2017 to June 2015. It would also change Section 501 of FISA.
- **H.R. 2399** (Conyers, The LIBERT-E Act): This bill would amend Section 501 of FISA to preclude the breadth of intelligence collection currently taking place. The bill also includes a new reporting requirement for requests made pursuant to Section 501.

Legislative proposals in the 112th Congress include:

- **S. 3515** (Merkley, Protect America's Privacy Act): A version of this bill introduced in the 112th Congress would have amended Section 702 of the Foreign Intelligence Surveillance Act to strengthen privacy protection for individuals inside the United States.

Author Contact Information

Marshall Curtis Erwin
Analyst in Intelligence and National Security
merwin@crs.loc.gov, 7-7739

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