

**ADMINISTRATION WHITE PAPER**

**BULK COLLECTION OF TELEPHONY METADATA  
UNDER SECTION 215 OF THE USA PATRIOT ACT**

August 9, 2013

## **BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT**

This white paper explains the Government’s legal basis for an intelligence collection program under which the Federal Bureau of Investigation (FBI) obtains court orders directing certain telecommunications service providers to produce telephony metadata in bulk. The bulk metadata is stored, queried and analyzed by the National Security Agency (NSA) for counterterrorism purposes. The Foreign Intelligence Surveillance Court (“the FISC” or “the Court”) authorizes this program under the “business records” provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted as section 215 of the USA PATRIOT Act (Section 215). The Court first authorized the program in 2006, and it has since been renewed thirty-four times under orders issued by fourteen different FISC judges. This paper explains why the telephony metadata collection program, subject to the restrictions imposed by the Court, is consistent with the Constitution and the standards set forth by Congress in Section 215. Because aspects of this program remain classified, there are limits to what can be said publicly about the facts underlying its legal authorization. This paper is an effort to provide as much information as possible to the public concerning the legal authority for this program, consistent with the need to protect national security, including intelligence sources and methods. While this paper summarizes the legal basis for the program, it is not intended to be an exhaustive analysis of the program or the legal arguments or authorities in support of it.

### **EXECUTIVE SUMMARY**

Under the telephony metadata collection program, telecommunications service providers, as required by court orders issued by the FISC, produce to the Government certain information about telephone calls, principally those made within the United States and between the United States and foreign countries. This information is limited to telephony metadata, which includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted. Importantly, this information does *not* include any information about the content of those calls—the Government cannot, through this program, listen to or record any telephone conversations.

This telephony metadata is important to the Government because, by analyzing it, the Government can determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States. The program is carefully limited to this purpose: it is not lawful for anyone to query the bulk telephony metadata for any purpose other than counterterrorism, and Court-imposed rules strictly limit all such queries. The program includes internal oversight mechanisms to prevent misuse, as well as external reporting requirements to the FISC and Congress.

Multiple FISC judges have found that Section 215 authorizes the collection of telephony metadata in bulk. Section 215 permits the FBI to seek a court order directing a business or other entity to produce records or documents when there are reasonable grounds to believe that the information sought is relevant to an authorized investigation of international terrorism. Courts have held in the analogous contexts of civil discovery and criminal and administrative

investigations that “relevance” is a broad standard that permits discovery of large volumes of data in circumstances where doing so is necessary to identify much smaller amounts of information within that data that directly bears on the matter being investigated. Although broad in scope, the telephony metadata collection program meets the “relevance” standard of Section 215 because there are “reasonable grounds to believe” that this category of data, when queried and analyzed consistent with the Court-approved standards, will produce information pertinent to FBI investigations of international terrorism, and because certain analytic tools used to accomplish this objective require the collection and storage of a large volume of telephony metadata. This does not mean that Section 215 authorizes the collection and storage of all types of information in bulk: the relevance of any particular data to investigations of international terrorism depends on all the facts and circumstances. For example, communications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism.

Moreover, information concerning the use of Section 215 to collect telephony metadata in bulk was made available to all Members of Congress, and Congress reauthorized Section 215 without change after this information was provided. It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the statute was reauthorized.

The telephony metadata collection program also complies with the Constitution. Supreme Court precedent makes clear that participants in telephone calls lack a reasonable expectation of privacy for purposes of the Fourth Amendment in the telephone numbers used to make and receive their calls. Moreover, particularly given the Court-imposed restrictions on accessing and disseminating the data, any arguable privacy intrusion arising from the collection of telephony metadata would be outweighed by the public interest in identifying suspected terrorist operatives and thwarting terrorist plots, rendering the program reasonable within the meaning of the Fourth Amendment. Likewise, the program does not violate the First Amendment, particularly given that the telephony metadata is collected to serve as an investigative tool in authorized investigations of international terrorism.

## **I. THE TELEPHONY METADATA COLLECTION PROGRAM**

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort. It is imperative that we have the capability to rapidly identify any terrorist threat inside the United States.

One important method that the Government has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the United States. The term “metadata” as used here refers to data collected under the program that is about telephone calls but does not include the content of those calls. By analyzing telephony metadata based on

telephone numbers or other identifiers associated with terrorist activity, trained expert analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the homeland. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are communicating with others inside the United States, as well as communications between operatives within the United States. In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.

Pursuant to Section 215, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce business records that contain information about communications between telephone numbers, generally relating to telephone calls made between the United States and a foreign country and calls made entirely within the United States. The information collected includes, for example, the telephone numbers dialed, other session-identifying information, and the date, time, and duration of a call. The NSA, in turn, stores and analyzes this information under carefully controlled circumstances. The judicial orders authorizing the collection do not allow the Government to collect the *content* of any telephone call, or the names, addresses, or financial information of any party to a call. The Government also does not collect cell phone locational information pursuant to these orders.

The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an “identifier,” such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a “seed.” Specifically, under Court-approved rules applicable to the program, there must be a “reasonable, articulable suspicion” that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. When the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. The “reasonable, articulable suspicion” requirement protects against the indiscriminate querying of the collected data. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

Information responsive to an authorized query could include, among other things, telephone numbers that have been in contact with the terrorist-associated number used to query the data, plus the dates, times, and durations of the calls. Under the FISC’s order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as “hops”). The first “hop” refers to the set of numbers directly in contact with the seed

identifier. The second “hop” refers to the set of numbers found to be in direct contact with the first “hop” numbers, and the third “hop” refers to the set of numbers found to be in direct contact with the second “hop” numbers. Following the trail in this fashion allows focused inquiries on numbers of interest, thus potentially revealing a contact at the second or third “hop” from the seed telephone number that connects to a different terrorist-associated telephone number already known to the analyst. Thus, the order allows the NSA to retrieve information as many as three “hops” from the initial identifier. Even so, under this process, only a tiny fraction of the bulk telephony metadata records stored at NSA are authorized to be seen by an NSA intelligence analyst, and only under carefully controlled circumstances.

Results of authorized queries are stored and are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata. Query results can be further analyzed only for valid foreign intelligence purposes. Based on this analysis of the data, the NSA then provides leads to the FBI or others in the Intelligence Community. For U.S. persons, these leads are limited to counterterrorism investigations. Analysts must also apply the minimization and dissemination requirements and procedures specifically set out in the Court’s orders before query results, in any form, are disseminated outside of the NSA. NSA’s analysis of query results obtained from the bulk metadata has generated and continues to generate investigative leads for ongoing efforts by the FBI and other agencies to identify and track terrorist operatives, associates, and facilitators.

Thus, critically, although a large amount of metadata is consolidated and preserved by the Government, the vast majority of that information is never seen by any person. Only information responsive to the limited queries that are authorized for counterterrorism purposes is extracted and reviewed by analysts. Although the number of unique identifiers has varied substantially over the years, in 2012, fewer than 300 met the “reasonable, articulable suspicion” standard and were used as seeds to query the data after meeting the standard. Because the same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three “hops” from the seed identifier, the number of metadata records responsive to such queries is substantially larger than 300, but it is still a tiny fraction of the total volume of metadata records. It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.

If the FBI investigates a telephone number or other identifier tipped to it through this program, the FBI must rely on publicly available information, other available intelligence, or other legal processes in order to identify the subscribers of any of the numbers that are retrieved. For example, the FBI could submit a grand jury subpoena to a telephone company to obtain subscriber information for a telephone number. If, through further investigation, the FBI were able to develop probable cause to believe that a number in the United States was being used by an agent of a foreign terrorist organization, the FBI could apply to the FISC for an order under Title I of FISA to authorize interception of the contents of future communications to and from that telephone number.

The telephony metadata collection program is subject to an extensive regime of oversight and internal checks and is monitored by the Department of Justice (DOJ), the FISC, and

Congress, as well as the Intelligence Community. No more than twenty-two designated NSA officials can make a finding that there is “reasonable, articulable suspicion” that a seed identifier proposed for query is associated with a specific foreign terrorist organization, and NSA’s Office of General Counsel must review and approve any such findings for numbers believed to be used by U.S. persons. In addition, before the NSA disseminates any information about a U.S. person outside the agency, a high-ranking NSA official must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance. Among the program’s additional safeguards and requirements are: (1) audits and reviews of various aspects of the program, including “reasonable, articulable suspicion” findings, by several entities within the Executive Branch, including NSA’s legal and oversight offices and the Office of the Inspector General, as well as attorneys from DOJ’s National Security Division and the Office of the Director of National Intelligence (ODNI); (2) controls on who can access and query the collected data; (3) requirements for training of analysts who receive the data generated by queries; and (4) a five-year limit on retention of raw collected data.

In addition to internal oversight, any compliance matters in this program that are identified by the NSA, DOJ, or ODNI are reported to the FISC. The FISC’s orders to produce records under the program must be renewed every 90 days, and applications for renewals must report information about how the authority has been implemented under the prior authorization. Significant compliance incidents are also reported to the Intelligence and Judiciary Committees of both houses of Congress. Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight. In accordance with the Court’s rules, upon discovery, these violations were reported to the FISC, which ordered appropriate remedial action. The incidents, and the Court’s responses, were also reported to the Intelligence and Judiciary Committees in great detail. These problems generally involved human error or highly sophisticated technology issues related to NSA’s compliance with particular aspects of the Court’s orders. The FISC has on occasion been critical of the Executive Branch’s compliance problems as well as the Government’s court filings. However, the NSA and DOJ have corrected the problems identified to the Court, and the Court has continued to authorize the program with appropriate remedial measures.

## **II. THE TELEPHONY METADATA COLLECTION PROGRAM COMPLIES WITH SECTION 215**

The collection of telephony metadata in bulk for counterterrorism purposes, subject to the restrictions identified above, complies with Section 215, as fourteen different judges of the FISC have concluded in issuing orders directing telecommunications service providers to produce the data to the Government. This conclusion does *not* mean that any and all types of business records—such as medical records or library or bookstore records—could be collected in bulk under this authority. In the context of communications metadata, in which connections between individual data points are important, and analysis of bulk metadata is the only practical means to find those otherwise invisible connections in an effort to identify terrorist operatives and networks, the collection of bulk data is relevant to FBI investigations of international terrorism.

This collection, moreover, occurs only in a context in which the Government’s acquisition, use, and dissemination of the information are subject to strict judicial oversight and rigorous protections to prevent its misuse.

## A. Statutory Requirements

Section 215 authorizes the FISC to issue an order for the “production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism,” except that it prohibits an “investigation of a United States person” that is “conducted solely on the basis of activities protected by the first amendment to the Constitution.” 50 U.S.C. § 1861(a)(1). The Government’s application for an order must include “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to [such] an authorized investigation (other than a threat assessment)” and that the investigation is being conducted under guidelines approved by the Attorney General. *Id.* § 1861(b)(2)(A) and (a)(2)(A). Because Section 215 does not authorize the FISC to issue an order for the collection of records in connection with FBI threat assessments,<sup>1</sup> to obtain records under Section 215 the investigation must be “predicated” (e.g., based on facts or circumstances indicative of terrorism, consistent with FBI guidelines approved by the Attorney General). Finally, Section 215 authorizes the collection of records only if they are of a type that could be obtained either “with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things.” *Id.* § 1861(c)(2)(D).<sup>2</sup> The telephony metadata collection program complies with each of these requirements.

**1. Authorized Investigation.** The telephony metadata records are sought for properly predicated FBI investigations into specific international terrorist organizations and suspected terrorists. The FBI conducts the investigations consistent with the *Attorney General’s Guidelines for Domestic FBI Operations*, U.S. Dep’t of Justice (2008), which direct the FBI “to protect the United States and its people from . . . threats to the national security” and to “further the foreign intelligence objectives of the United States,” a mandate that extends beyond traditional criminal law enforcement. *See id.* at 12. The guidelines authorize a full investigation into an international terrorist organization if there is an “articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged . . . in . . . international terrorism or other threat to the national security,” or may be planning or

---

<sup>1</sup> “Threat assessments” refer to investigative activity that does not require any particular factual predication (but does require an authorized purpose and cannot be based on the exercise of First Amendment protected activity or on race, ethnicity, national origin, or religion of the subject). *FBI Domestic Investigations and Operations Guide*, § 5.1 (2011).

<sup>2</sup> Indeed, Section 215 was enacted because the FBI lacked the ability, in national security investigations, to seek business records in a way similar to its ability to seek records using a grand jury subpoena in a criminal case or an administrative subpoena in civil investigations. *See, e.g.*, S. Rep. No. 109-85, at 20 (2005) (“[A] federal prosecutor need only sign and issue a grand jury subpoena to obtain similar documents in criminal investigations, yet national security investigations have no similar investigative tool.”).

supporting such conduct. *See id.* at 23. FBI investigations into the international terrorist organizations identified to the Court readily meet that standard, and there have been numerous FBI investigations in the last several years to which the telephony metadata records are relevant. The guidelines provide that investigations of a terrorist organization “may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; [and] the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives.” *Id.* And in investigating international terrorism, the FBI is *required* to “fully utilize the authorities and the methods authorized” in the guidelines, which include “[a]ll lawful . . . methods,” including the use of intelligence tools such as Section 215. *Id.* at 12 and 31.

**2. Tangible Things.** The telephony metadata records are among the types of materials that can be obtained under Section 215. The statute broadly provides for the production of “any tangible things (including books, records, papers, documents, and other items).” *See* 50 U.S.C. § 1861(a)(1). There is little question that in enacting Section 215 in 2001 and then amending it in 2006, Congress understood that among the things that the FBI would need to acquire to conduct terrorism investigations were documents and records stored in electronic form. Congress may have used the term “tangible things” to make clear that this authority covers the production of items as opposed to oral testimony, which is another type of subpoena beyond the scope of Section 215. Thus, as Congress has made clear in other statutes involving production of records, “tangible things” include electronically stored information. *See* 7 U.S.C. § 7733(a) (“The Secretary shall have the power to subpoena . . . the production of all evidence (including books, papers, documents, electronically stored information, and *other* tangible things that constitute or contain evidence.”) (emphasis added); 7 U.S.C. § 8314 (a)(2)(A) (containing the same language).<sup>3</sup>

The non-exhaustive list of “tangible things” in Section 215, moreover, includes the terms “documents” and “records,” both of which are commonly used in reference to information stored in electronic form. The telephony metadata information is an electronically stored “record” of, among other information, the date, time, and duration of a call between two telephone numbers. And in the analogous context of civil discovery, the term “documents” has for decades been interpreted to include electronically stored information. The Federal Rules of Civil Procedure were amended in 1970 to make that understanding of the term “documents” explicit, *see Nat’l. Union Elec. Corp. v. Matsushita Elec. Indus. Co., Ltd.*, 494 F. Supp. 1257, 1261-62 (E.D. Pa. 1980), and again in 2006 to expressly add the term “electronically stored information.” *See* Fed. R. Civ. Pro. 34 (governing production of “documents, electronically stored information, and tangible things”).<sup>4</sup> Moreover, a judge may grant an order for production of records under

---

<sup>3</sup> The word “tangible” can be used in some contexts to connote not only tactile objects like pieces of paper, but also any other things that are “capable of being perceived” by the senses. *See Merriam Webster Online Dictionary* (2013) (defining “tangible” as “capable of being perceived *especially* by the sense of touch”) (emphasis added).

<sup>4</sup> The notes of the Advisory Committee on the 2006 amendments to Rule 34 explain that:

Lawyers and judges interpreted the term “documents” to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all



Section 215 only if the records could “be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of *records or tangible things*,” and grand jury subpoenas can be and frequently are used to seek electronically stored telephony metadata records such as those sought under Section 215 or other electronically stored records. *See* 50 U.S.C. § 1861(c)(2)(D) (emphasis added); 18 U.S.C. § 2703(b)(1)(B)(i). That further confirms that Section 215 applies to electronically stored information.<sup>5</sup>

**3. *Relevance to an Authorized Investigation.*** The telephony metadata program also satisfies the statutory requirement that there be “reasonable grounds to believe” that the records collected are “relevant to an authorized investigation . . . to obtain foreign intelligence information . . . or to protect against international terrorism or clandestine intelligence activities.” *See* 50 U.S.C. § 1861(b)(2)(A). The text of Section 215, considered in light of the well-developed understanding of “relevance” in the context of civil discovery and criminal and administrative subpoenas, as well as the broader purposes of this statute, indicates that there are “reasonable grounds to believe” that the records at issue here are “relevant to an authorized investigation.” Specifically, in the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information—and that it is necessary to collect a large volume of data in order

---

forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a ‘document.’ Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended *to confirm* that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change *clarifies* that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. *At the same time, a Rule 34 request for production of ‘documents’ should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and ‘documents.’*

Fed. R. Civ. Pro 34, Notes of Advisory Committee on 2006 Amendments (emphasis added).

<sup>5</sup> The legislative history of Section 215 also supports this reading of the provision to include electronic data. In its discussion of Section 215, the House Report accompanying the USA PATRIOT Reauthorization Act of 2006 notes that there were electronic records in a Florida public library that might have been used to help prevent the September 11, 2001, attacks had the FBI obtained them. *See* H.R. Rep. No. 109-174(I), at 17-18 (2005). Specifically, the report describes “records indicat[ing] that a person using [the hijacker] Alhazmi’s account used the library’s computer to review September 11th reservations that had been previously booked.” *Id.* at 18. Congress used this example to illustrate the types of “tangible things” that Section 215 authorizes the FBI to obtain through a FISC order. Moreover, the House Report cites testimony in 2005 by the Attorney General before the House Committee on the Judiciary, where the Attorney General explained that Section 215 had been used “to obtain driver’s license records, public accommodation records, apartment leasing records, credit card records, *and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen-register devices.*” *Id.* (emphasis added). Telecommunications service providers store such subscriber information electronically. Accordingly, the House Report suggests that Congress understood that Section 215 had been used to capture electronically stored records held by telecommunications service providers and reauthorized Section 215 based on that understanding.

to employ the analytic tools needed to identify that information—the standard of relevance under Section 215 is satisfied.

Standing alone, “relevant” is a broad term that connotes anything “[b]earing upon, connected with, [or] pertinent to” a specified subject matter. 13 Oxford English Dictionary 561 (2d ed. 1989). The concept of relevance, however, has developed a particularized legal meaning in the context of the production of documents and other things in conjunction with official investigations and legal proceedings. Congress legislated against that legal background in enacting Section 215 and thus “presumably kn[ew] and adopt[ed] the cluster of ideas that were attached to [the] word in the body of learning from which it was taken.” See *FAA v. Cooper*, 132 S. Ct. 1441, 1449 (2012) (internal citation and quotation marks omitted). Indeed, as discussed above, in identifying the sort of items that may be the subject of a Section 215 order, Congress expressly referred to items obtainable with “a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation” or “any other order issued by a court of the United States directing the production of records or tangible things,” 50 U.S.C. § 1861(c)(2)(D), indicating that it was well aware of this legal context when it added the relevance requirement. That understanding is also reflected in the statute’s legislative history. See 152 Cong. Rec. 2426 (2006) (statement of Sen. Kyl) (“Relevance is a simple and well established standard of law. Indeed, it is the standard for obtaining every other kind of subpoena, including administrative subpoenas, grand jury subpoenas, and civil discovery orders.”).

It is well-settled in the context of other forms of legal process for the production of documents that a document is “relevant” to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter. In civil discovery, for example, the Supreme Court has construed the phrase “relevant to the subject matter involved in the pending action” “broadly to encompass 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.” *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (emphasis added); see also *Condit v. Dunne*, 225 F.R.D. 100, 105 (S.D.N.Y. 2004) (“Although not unlimited, relevance, for purposes of discovery, is an extremely broad concept.”). A similar standard applies to grand jury subpoenas, which will be upheld unless “there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury’s investigation.” *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).<sup>6</sup> And the Supreme Court has explained that a statutory “relevance” limitation on administrative subpoenas, even for investigations into matters not involving national security threats, is “not especially constraining” and affords an agency “access to virtually any material that might cast light on the allegations” at issue in an investigation. *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984). See also *United*

---

<sup>6</sup> One court has noted that the Court’s reference to “category of materials,” rather than to specific documents, “contemplates that the district court will assess relevancy based on the broad types of material sought by the Government,” not by “engaging in a document-by-document [or] line-by-line assessment of relevancy.” *In re Grand Jury Proceedings*, 616 F.3d 1186, 1202 (10th Cir. 2010). The court explained that “[i]ncidental production of irrelevant documents . . . is simply a necessary consequence of the grand jury’s broad investigative powers and the categorical approach to relevancy adopted in *R. Enterprises*.” *Id.* at 1205.

*States v. Arthur Young & Co.*, 465 U.S. 805, 814 (1984) (stating that IRS’s statutory power to subpoena any records that may be relevant to a particular tax inquiry allows IRS to obtain items “of even *potential* relevance to an ongoing investigation”) (emphasis in original). Relevance in that context is not evaluated in a vacuum but rather through consideration of the nature, purpose, and scope of the investigation, *see, e.g., Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946), and courts generally defer to an agency’s appraisal of what is relevant. *See, e.g., EEOC v. Randstad*, 685 F.3d 433, 451 (4th Cir. 2012).

In light of that basic understanding of relevance, courts have held that the relevance standard permits requests for the production of 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.<sup>7</sup> More generally, courts have concluded that the relevance standard permits discovery of large volumes of information in circumstances where the requester seeks to identify much smaller amounts of information within the data that directly bears on the matter.<sup>8</sup> Federal agencies exercise broad subpoena powers or other authorities to collect and analyze large data sets in order to identify information that directly pertains to the particular subject of an investigation.<sup>9</sup> Finally, in the analogous field of search warrants for data stored on computers, courts permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B) (“A warrant . . . may

---

<sup>7</sup> *See, e.g., Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at \*2 (S.D. Cal. Feb. 11, 2011) (holding that there is reason to believe that law firm’s trust account information for all of its clients is relevant to SEC investigation, where the Government asserted the trust account information “may reveal concealed connections between unidentified entities and persons and those identified in the investigation thus far . . . [and] the transfer of funds cannot effectively be traced without access to all the records.”); *Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC*, 2007 WL 3492762 at \*1 (N.D. Ga. Nov. 5, 2007) (compelling production of business’s entire underwriting database, despite business’s assertion that it contained a significant amount of irrelevant data); *see also Chen-Oster v. Goldman, Sachs & Co.*, 285 F.R.D. 294, 305 (S.D.N.Y. 2012) (noting that production of multiple databases could be ordered as a “data dump” if necessary for plaintiffs’ statistical analysis of business’s employment practices).

<sup>8</sup> *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000) (holding that subpoena to doctor to produce 15,000 patient files was relevant to investigation of doctor for healthcare fraud); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (upholding grand jury subpoenas for all wire money transfer records of business’s primary wire service agent in the Kansas City area that exceeded \$1000 for a one year period despite claim that “the subpoena may make available to the grand jury records involving hundreds of innocent people”); *In re Adelpia Comm. Corp.*, 338 B.R. 546, 549 and 553 (Bankr. S.D.N.Y. 2005) (permitting inspection of “approximately 20,000 large bankers boxes of business records,” and holding that “[i]t is well-settled . . . that sheer volume alone is an insufficient reason to deny discovery of documents”); *Medtronic Sofamor Danek, Inc. v. Michelson*, 229 F.R.D. 550, 552 (W.D. Tenn. 2003) (concerning discovery request for “approximately 996 network backup tapes, containing, among other things, electronic mail, plus an estimated 300 gigabytes of other electronic data that is not in a backed-up format, all of which contains items potentially responsive to discovery requests”).

<sup>9</sup> *See, e.g., F.T.C. v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992) (upholding broad subpoena for financial information in FTC investigation of unfair or deceptive trade practices because it “could facilitate the Commission’s investigation . . . in different ways, not all of which may yet be apparent”); *see also Associated Container Transp. (Aus.) Ltd. v. United States*, 705 F.2d 53, 58 (2nd Cir. 1983) (“recognizing the broad investigatory powers granted to the Justice Department by the Antitrust Civil Process Act,” which are broad in scope due to the “less precise nature of investigations”) (quoting H.R. Rep. No. 94-1343, at 11 (1976)).

authorize the seizure of electronic storage media ... [and] authorize[] a later review of the media or information consistent with the warrant.”).<sup>10</sup> These longstanding practices in a variety of legal arenas demonstrate a broad understanding of the requirement of relevance developed in the context of investigatory information collection.

It is reasonable to conclude that Congress had that broad concept of relevance in mind when it incorporated this standard into Section 215. The statutory relevance standard in Section 215, therefore, should be interpreted to be at least as broad as the standard of relevance that has long governed ordinary civil discovery and criminal and administrative investigations, which allows the broad collection of records when necessary to identify the directly pertinent documents. To be sure, the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program, and the purpose for which information was sought in these cases was not as expansive in scope as a nationwide intelligence collection effort designed to identify terrorist threats. While these cases do *not* demonstrate that bulk collection of the type at issue here would routinely be permitted in civil discovery or a criminal or administrative investigation, they do show that the “relevance” standard affords considerable latitude, where necessary, and depending on the context, to collect a large volume of data in order to find the key bits of information contained within. Moreover, there are a number of textual and contextual indications that Congress intended Section 215 to embody an even more flexible standard that takes into account the uniquely important purposes of the statute, the factual environment in which national security investigations take place, and the special facets of the statutory scheme in which Section 215 is embedded.

First, Section 215’s standard on its face is particularly broad, because the Government need only show that there are “reasonable grounds to believe” that the records sought are relevant to an authorized investigation. 50 U.S.C. § 1861(b)(2)(A). That phrase reflects Congress’s understanding that Section 215 permits a particularly broad scope for production of records in connection with an authorized national security investigation.<sup>11</sup>

Second, unlike, for example, civil discovery rules, which limit discovery to those matters “relevant to the subject matter involved in the action,” Fed. R. Civ. P. 26(b)(1), Section 215 requires only that the documents be relevant to an “authorized *investigation*.” 50 U.S.C.

---

<sup>10</sup> See, e.g., *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006) (recognizing that “blanket seizure” of the defendant’s entire computer system, followed by subsequent review, may be permissible if explanation as to why it is necessary is provided); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (explaining that “the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images” and that “[a] sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application”).

<sup>11</sup> Some Members of Congress opposed Section 215 because in their view it afforded too broad a standard for collection of information. See, e.g., 152 Cong. Rec. 2422 (2006) (statement of Sen. Feingold) (“[T]he deal would allow subpoenas in instances when there are reasonable grounds for simply believing that information is relevant to a terrorism investigation. That is an extremely low bar.”); 156 Cong. Rec. S2108-01 (2010) (statement of Sen. Wyden) (“‘Relevant’ is an incredibly broad standard. In fact, it could potentially permit the Government to collect the personal information of large numbers of law-abiding Americans who have no connection to terrorism whatsoever.”)

§ 1861(b)(2)(A) (emphasis added). This includes not only information directly relevant to the authorized object of the investigation—*i.e.*, “foreign intelligence information” or “international terrorism or clandestine intelligence activities”—but also information relevant to the investigative process or methods employed in reasonable furtherance of such national security investigations. In the particular circumstance in which the collection of communications metadata in bulk is necessary to enable discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity, the metadata records are relevant to the FBI’s “investigation[s]” to which those connections relate. Notably, Congress *specifically rejected* proposals to limit the relevance standard so that it would encompass only records pertaining to individuals suspected of terrorist activity.<sup>12</sup>

Third, unlike most civil or criminal discovery or administrative inquiries, these investigations often focus on *preventing* threats to national security from causing harm, not on the retrospective determination of liability or guilt for prior activities. The basic purpose of Section 215, after all, is to provide a tool for discovering and thwarting terrorist plots and other national security threats that may not be known to the Government at the outset. For that reason, Congress recognized that in collecting records potentially “relevant to an authorized investigation” under Section 215, the FBI would not be limited to records known with certainty, or even with a particular level of statistical probability, to contain information that directly bears on a terrorist plot or national security threat. Rather, for Section 215 to be effective in advancing its core objective, the FBI must have the authority to collect records that, when subjected to reasonable and proven investigatory techniques, can produce information that will help the Government to identify previously unknown operatives and thus to prevent terrorist attacks before they succeed.

Fourth, and relatedly, unlike ordinary criminal investigations, the sort of national security investigations with which Section 215 is concerned often have a remarkable breadth—spanning long periods of time, multiple geographic regions, and numerous individuals, whose identities are often unknown to the intelligence community at the outset. The investigative tools needed to combat those threats must be deployed on a correspondingly broad scale. In this context, it is not surprising that Congress enacted a statute with a standard that enables the FBI to seek certain

---

<sup>12</sup> See S. 2369, 109th Cong. § 3 (2006) (requiring Government to demonstrate relevance of records sought to agents of foreign powers, including terrorist organizations, or their activities or contacts); 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin) (“The Senate bill required a showing that the records sought were not only relevant to an investigation but also either pertained to a foreign power or an agent of a foreign power, which term includes terrorist organizations, or were relevant to the activities of a suspected agent of a foreign power who is the subject of an authorized investigation or pertained to an individual in contact with or known to be a suspected agent. In other words, the order had to be linked to some suspected individual or foreign power. Those important protections are omitted in the bill before us.”); 152 Cong. Rec. H581-02 (2006) (statement of Rep. Nadler) (“The conference report does not restore the section 505 previous standard of specific and articulable facts connecting the records sought to a suspected terrorist. It should.”); 151 Cong. Rec. S14275-01 (2005) (statement of Sen. Dodd) (“Unfortunately, the conference report differs from the Senate version as it maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, suspected of terrorist activity. Additionally, the conference report does not impose any limit on the breadth of the records that can be requested or how long these records can be kept by the Government.”).

records in bulk where necessary to identify connections between individuals suspected to be involved in terrorism.

Fifth, Congress built into the statutory scheme protections not found in the other legal contexts to help ensure that even an appropriately broad construction of the “relevance” requirement will not lead to misuse of the authority. Section 215, unlike the rules governing civil discovery or grand jury subpoenas, always requires prior judicial approval of the Government’s assertion that particular records meet the relevance requirement and the other legal prerequisites. Once the information is produced, the Government can retain and disseminate the information only in accordance with minimization procedures reported to and approved by the Court. *See* 50 U.S.C. § 1861(g). The entire process is subject to active congressional oversight. *See, e.g., id.* § 1862. Although Congress certainly intended the Government to make a threshold showing of relevance before obtaining information under Section 215, these more robust protections regarding collection, retention, dissemination, and oversight provide additional mechanisms for promoting responsible use of the authority.

In light of these features of Section 215, and the broad understanding of “relevance,” the telephony metadata collection program meets the Section 215 “relevance” standard. There clearly are “reasonable grounds to believe” that this category of data, when queried and analyzed by the NSA consistent with the Court-imposed standards, will produce information pertinent to FBI investigations of international terrorism, and it is equally clear that NSA’s analytic tools require the collection and storage of a large volume of metadata in order to accomplish this objective. As noted above, NSA employs a multi-tiered process of analyzing the data in an effort to identify otherwise unknown connections between telephone numbers associated with known or suspected terrorists and other telephone numbers, and to analyze those connections in a way that can help identify terrorist operatives or networks. That process is not feasible unless NSA analysts have access to telephony metadata in bulk, because they cannot know which of the many phone numbers might be connected until they conduct the analysis. The results of the analysis ultimately can assist in discovering whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, including persons and activities inside the United States. If not collected and held by the NSA, telephony metadata may not continue to be available for the period of time (currently five years) deemed appropriate for national security purposes because telecommunications service providers are not typically required to retain it for this length of time. Unless the data is aggregated, it may not be feasible to identify chains of communications that cross different telecommunications networks. Although NSA is exploring whether certain functions could be performed by the telecommunications service providers, doing so may not be possible without significant additional investment and new statutes or regulations requiring providers to preserve and format the records and render necessary technical assistance.

The national security objectives advanced by the telephony metadata program would therefore be frustrated if the NSA were limited to collection of a narrower set of records. In particular, a more restrictive collection of telephony metadata would impede the ability to identify a chain of contacts between telephone numbers, including numbers served by different telecommunications service providers, significantly curtailing the usefulness of the tool. This is therefore not a case in which a broad collection of records provides only a marginal increase in

the amount of useful information generated by the program. Losing the ability to conduct focused queries on bulk metadata would significantly diminish the effectiveness of NSA's investigative tools. As discussed above, the broad meaning of the relevance standard that Congress incorporated into Section 215 encompasses, in this particular circumstance, collection of a repository of information without which the Government might not be able to identify specific information that bears directly on a counterterrorism investigation. For that reason, the telephony metadata records are "relevant" to an authorized investigation of international terrorism.

This conclusion does not mean that the scope of Section 215 is boundless and authorizes the FISC to order the production of every type of business record in bulk—including medical records or library or book sale records, for example. As noted above, the Supreme Court has explained that determining the appropriate scope of a subpoena for the production of records "cannot be reduced to formula; for relevancy and adequacy or excess in the breadth of [a] subpoena are matters variable in relation to the nature, purposes and scope of the inquiry." *Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946). In other contexts, the FISC might not conclude that collection of records in bulk meets the "relevance" standard because of the nature of the records at issue and the extent to which collecting such records in large volumes is necessary in order to produce information pertinent to investigations of international terrorism. For example, the Government's ability to analyze telephony metadata, including through the techniques discussed above, to discover connections between individuals fundamentally distinguishes such data from medical records or library records. Although an identified suspect's medical history might be relevant to an investigation of that individual, searching an aggregate database of medical records—which do not interconnect to one another—would not typically enable the Government to identify otherwise unknown relationships among individuals and organizations and therefore to ascertain information about terrorist networks. Moreover, given the frequent use of the international telephone system by terrorist networks and organizations, analysis of telephony metadata in bulk is a potentially important means of identifying terrorist operatives, particularly those persons who may be plotting terrorist attacks within the United States. Although there could be individual contexts in which the Government has an interest in obtaining medical records or library records for counterterrorism purposes, these categories of data are not in general comparable to communications metadata as a means of identifying previously unknown terrorist operatives or networks. The potential need for communications metadata is both persistent and pervasive across numerous counterterrorism investigations in a way that is not applicable to many other types of data. Communications metadata therefore presents a context in which using sophisticated analytic tools can be important to many investigations of international terrorism, and the use of those tools in turn requires collection of a large volume of data to be effective.

Under the telephony metadata program, the statutory requirement for judicial authorization serves as a check to focus Government investigations only on that information most likely to facilitate an authorized investigation. Under the FISC's orders, the amount of metadata actually reviewed by the Government is narrow. As noted above, those orders require, among other things, that NSA analysts have reasonable, articulable suspicion that the seed identifiers, such as telephone numbers, they submit to query the data are associated with specific foreign terrorist organizations that have previously been identified to and approved by the Court.

The vast majority of the telephony metadata is never seen by any person because it is not responsive to the limited queries that are authorized. But the information that is generated in response to these limited queries could be especially significant in helping the Government identify and disrupt terrorist plots. Thus, while the relevance standard provides the Government with broad authority to collect data that is necessary to conduct authorized investigations, the FISC's orders require that the data will be substantively queried *only* for that authorized purpose. That is the balanced scheme that Congress adopted when it joined the broad relevance standard with the requirement for judicial approval set forth in Section 215.

Indeed, given the rigorous protections imposed by the FISC, even if the statutory standard were not "relevance" as the term has been used in analogous legal contexts, but rather the Fourth Amendment reasonableness standard that the Supreme Court has adopted for searches not predicated on individualized suspicion, the telephony metadata program would be lawful. (For the reasons discussed below, the Fourth Amendment's reasonableness requirement does not apply in this context because individuals have no reasonable expectation of privacy in the telephony metadata records collected from providers under the program, *see pp. 19-21, infra*, but for present purposes we assume contrary to the facts that such a reasonable expectation exists.) The Supreme Court has held that "where a Fourth Amendment intrusion serves special government needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or . . . individualized suspicion in the particular context." *Nat'l Treas. Employees Union v. Von Raab*, 489 U.S. 656, 665-66 (1989). As noted above, the telephony metadata collected under Section 215 does not include the private content of any person's telephone calls, or who places or answers the calls, but only technical data, such as information concerning the numbers dialed and the time and duration of the calls. Even if there were an individual privacy interest in such telephony metadata under the Fourth Amendment, it would be limited, and any infringement on that interest would be substantially mitigated by the judicially approved restrictions on accessing and disseminating the data. *See Board of Educ. of Indep. School Dist. No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822, 833 (2002) (finding that restrictions on access to drug testing information lessened testing program's intrusion on privacy). On the other side of the scale, the interest of the Government—and the broader public—in discovering and tracking terrorist operatives and thwarting terrorist attacks is a national security concern of overwhelming importance. *See Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); *see also In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) ("Here, the relevant governmental interest—the interest in national security—is of the highest order of magnitude."). Moreover, the telephony metadata collection program is, at the very least, "a reasonably effective means of addressing" the Government's national security needs in this context. *Earls*, 536 U.S. at 837. Thus, even if the appropriate standard for the telephony metadata collection program were not relevance, but rather a Fourth Amendment reasonableness analysis, the Government's interest is compelling and immediate, the intrusion on privacy interests is limited, and the collection is a reasonably effective means of detecting and monitoring terrorist operatives and thereby obtaining information important to FBI investigations.



**4. Prospective Orders.** Section 215 authorizes the FISC to issue orders to produce telephony metadata records prospectively. Nothing in the text of the statute suggests that FISC orders may relate only to records previously created. The fact that the requested information has not yet been created at the time of the application, and that its production is requested on an ongoing basis, does not affect the basic character of the information as “documents,” “records,” or other “tangible things” subject to production under the statute. Nor do the orders require the creation or preservation of documents that would otherwise not exist. Section 215 orders are not being used to compel a telecommunications service provider to retain information that the provider would otherwise discard, because the telephony metadata records are routinely maintained by the providers for at least eighteen months in the ordinary course of business pursuant to Federal Communications Commission regulations. *See* 47 C.F.R. § 42.6. In this context, the continued existence of the records and their continuing relevance to an international terrorism investigation will not change over the 90-day life of a FISC order.

Prospective production of records has been deemed appropriate in other analogous contexts. For example, courts have held that the Federal Rules of Civil Procedure give a court the “authority to order [the] respondent to produce materials created after the return date of the subpoena.” *Chevron v. Salazar*, 275 F.R.D. 437, 449 (S.D.N.Y. 2011); *see also United States v. I.B.M.*, 83 F.R.D. 92, 96 (S.D.N.Y. 1979). Other courts have held that, under the Stored Communications Act, because the statute does not “limit the ongoing disclosure of records to the Government as soon as they are created,” the Government may seek prospective disclosure of records. *See, e.g., In re Application for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008) (“prospective . . . information sought by the Government . . . becomes a ‘historical record’ as soon as it is recorded by the provider.”). Neither Section 215 nor any other part of the FISA statutory scheme prohibits the ongoing production of business records that are generated on a daily basis to the Government soon after they are created. Nor is there any legislative history indicating that Congress intended to prevent courts from issuing prospective orders under Section 215 in these circumstances.

This type of prospective order also provides efficient administration for all parties involved—the Court, the Government, and the provider. There is little doubt that the Government could seek a new order on a daily basis for the records created within the last 24 hours. But the creation and processing of such requests would impose entirely unnecessary burdens on both the Court and the Government—and no new information would be anticipated in such a short period of time to alter the basis of the Government’s request or the facts upon which the Court has based its order. Providers would also be forced to review daily requests of differing docket numbers, rather than merely complying with one ongoing request, which would be more onerous on the providers and raise potential and unnecessary compliance issues. Importantly, the FISC orders do not allow the Government to receive this information in perpetuity: the 90-day renewal requires the Government to make continuing justifications for the business records on a routine basis. Therefore, the prospective orders merely ensure that the records can be sought in a reasonable manner for a reasonable period of time while avoiding unreasonable and burdensome paperwork.

## B. Congressional Reauthorizations

The telephony metadata collection program satisfies the plain text and basic purposes of Section 215 (as well as the Constitution, *see infra* pp. 20-24) and is therefore lawful. But to the extent there is any question as to the program's compliance with the statute, it is significant that, after information concerning the telephony metadata collection program carried out under the authority of Section 215 was made available to Members of Congress, Congress twice reauthorized Section 215. When Congress reenacts a statute without change, it is presumed to have adopted the administrative or judicial interpretation of the statute if it is aware of the interpretation. *See Lorillard v. Pons*, 434 U.S. 575, 580 (1978). The FISC's conclusion that Section 215 authorized the collection of telephony metadata in bulk was classified and not publicly known. However, it is important to the legal analysis of the statute that the Congress was on notice of this program and the legal authority for it when the statute was reauthorized.

Although the proceedings before the FISC are classified, Congress has enacted legislation to ensure that its members are aware of significant interpretations of law by the FISC. FISA requires "the Attorney General [to] submit to the [Senate and House Intelligence and Judiciary Committees] . . . a summary of significant legal interpretations of this chapter involving matters before the [FISC or Foreign Intelligence Surveillance Court of Review (FISCR)], including interpretations presented in applications or pleadings filed with the [FISC or FISCR] by the Department of Justice and . . . copies of all decisions, orders, or opinions of the [FISC or FISCR] that include significant construction or interpretation of the provisions of this chapter." 50 U.S.C. § 1871(a). The Executive Branch not only complied with this requirement with respect to the telephony metadata collection program, it also worked to ensure that *all* Members of Congress had access to information about this program and the legal authority for it. Congress was thus on notice of the FISC's interpretation of Section 215, and with that notice, twice extended Section 215 without change.

In December 2009, DOJ worked with the Intelligence Community to provide a classified briefing paper to the House and Senate Intelligence Committees that could be made available to all Members of Congress regarding the telephony metadata collection program. A letter accompanying the briefing paper sent to the House Intelligence Committee specifically stated that "it is important that all Members of Congress have access to information about this program" and that "making this document available to all members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215." *See* Letter from Assistant Attorney General Ronald Weich to the Honorable Silvestre Reyes, Chairman, House Permanent Select Committee on Intelligence (Dec. 14, 2009). Both Intelligence Committees made this document available to all Members of Congress prior to the February 2010 reauthorization of Section 215. *See* Letter from Sen. Diane Feinstein and Sen. Christopher S. Bond to Colleagues (Feb. 23, 2010); Letter from Rep. Silvestre Reyes to Colleagues (Feb. 24, 2010); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden) ("[T]he Attorney General and the Director of National Intelligence have prepared a classified paper that contains details about how some of the Patriot Act's authorities have actually been used, and this paper is now available to all members of Congress, who can read it in the Intelligence Committee's secure office spaces. I would certainly encourage all of my colleagues to come down to the Intelligence

Committee and read it.”). That briefing paper, which has since been released to the public in redacted form, explained that the Government and the FISC had interpreted Section 215 to authorize the collection of telephony metadata in bulk.<sup>13</sup>

Additionally, the classified use of this authority has been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, including in connection with reauthorization efforts. Several Members of Congress have publicly acknowledged that the Executive Branch extensively briefed these committees on the telephony metadata collection program and that, beyond what is required by law, the Executive Branch also made available to all Members of Congress information about this program and its operation under Section 215.<sup>14</sup> Moreover, in early 2007, the Department of Justice began providing all significant FISC pleadings and orders related to this program to the Senate and House Intelligence and Judiciary committees. By December 2008, all four committees had received the initial application and primary order authorizing the telephony metadata collection. Thereafter, all pleadings and orders reflecting significant legal developments regarding the program were produced to all four committees.

After receiving the classified briefing papers, which were expressly designed to inform Congress’ deliberations on reauthorization of Section 215, Congress twice reauthorized this statutory provision, in 2010 and again in 2011. These circumstances provide further support to the FISC’s interpretation of Section 215 as authorizing orders directing the production of telephony metadata records in bulk, as well as the Executive Branch’s administrative construction of the statute to the same effect. *See Shell Oil Co.*, 466 U.S. at 69 (“Congress undoubtedly was aware of the manner in which the courts were construing the concept of ‘relevance’ and implicitly endorsed it by leaving intact the statutory definition of the

---

<sup>13</sup> An updated version of the briefing paper, also recently released in redacted form to the public, was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year. *See Letter from Assistant Attorney General Ronald Weich to the Honorable Dianne Feinstein and the Honorable Saxby Chambliss, Chairman and Vice Chairman, Senate Select Committee on Intelligence (Feb. 2, 2011); Letter from Assistant Attorney General Ronald Weich to the Honorable Mike Rogers and the Honorable C.A. Dutch Ruppersberger, Chairman and Ranking Minority Member, House Permanent Select Committee on Intelligence (Feb. 2, 2011)*. The Senate Intelligence Committee made this updated paper available to all Senators later that month. *See Letter from Sen. Diane Feinstein and Sen. Saxby Chambliss to Colleagues (Feb. 8, 2011)*.

<sup>14</sup> *See, e.g.*, Press Release of Senate Select Committee on Intelligence, *Feinstein, Chambliss Statement on NSA Phone Records Program* (June 6, 2013) (“The executive branch’s use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each reauthorization of this law.”); *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence*, 113 Cong. (2013) (statements of Rep. Rogers and Rep. Ruppersberger, Chair and Ranking Member, H. Permanent Select Comm. on Intelligence) (confirming extensive executive branch briefings for HPSCI on the telephony metadata collection program); Michael McAuliff & Sabrina Siddiqui, *Harry Reid: If Lawmakers Don’t know about NSA Surveillance, It’s Their Fault*, Huffington Post, June 11, 2013, available at [www.huffingtonpost.com/2013/06/11/harry-reid-nsa\\_n\\_3423393.html](http://www.huffingtonpost.com/2013/06/11/harry-reid-nsa_n_3423393.html) (quoting Sen. Reid) (“For senators to complain that ‘I didn’t know this was happening,’ we’ve had many, many meetings . . . that members have been invited to. . . [T]hey’ve had every opportunity to be aware of these programs.”)

Commission’s investigative authority.”); *Haig v. Agee*, 453 U.S. 280, 297-98 (1981) (finding that where Congress used language identical to that in an earlier statute and there was “no evidence of any intent to repudiate the longstanding administrative construction” of the earlier statute, the Court would “conclude that Congress . . . adopted the longstanding administrative construction” of the prior statute); *Atkins v. Parker*, 472 U.S. 115, 140 (1985) (“Congress was thus well aware of, and legislated on the basis of, the contemporaneous administrative practice . . . and must be presumed to have intended to maintain that practice absent some clear indication to the contrary.”) (citing *Haig*, 453 U.S. 297-98).<sup>15</sup>

### **III. THE TELEPHONY METADATA COLLECTION PROGRAM IS CONSTITUTIONAL**

The telephony metadata collection program also complies with the Constitution. Supreme Court precedent makes clear that participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the metadata records generated by their telephone calls and held by telecommunications service providers. Moreover, any arguable privacy intrusion arising from the collection of telephony metadata would be outweighed by the critical public interest in identifying connections between terrorist operatives and thwarting terrorist plots, rendering the program reasonable within the meaning of the Fourth Amendment. The program is also consistent with the First Amendment, particularly given that the database may be used only as an investigative tool in authorized investigations of international terrorism.

#### **A. Fourth Amendment**

A Section 215 order for the production of telephony metadata is not a “search” as to any individual because, as the Supreme Court has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the Government’s collection of dialed telephone numbers from a telephone company did not constitute a search of the petitioner under the Fourth Amendment, because persons making phone calls lack a reasonable expectation of privacy in the numbers they call. *Id.* at 743-46.

---

<sup>15</sup> Moreover, in both 2009 and 2011, when the Senate Judiciary Committee was considering possible amendments to Section 215, it made clear that it had no intention of affecting the telephony metadata collection program that had been approved by the FISC. The Committee reports accompanying the USA PATRIOT Act Sunset Extension Acts of 2009 and 2011 explained that proposed changes to Section 215 were “not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities.” S. Rep. No. 111-92, at 7 (2009); S. Rep. No. 112-13, at 10 (2011). Ultimately, Section 215 and other expiring provisions of the USA PATRIOT Act were extended to June 1, 2015 without change. *See* Patriot Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011). Likewise, Senators in the minority expressed the desire not to interfere with any activities carried out under Section 215 that had been approved by the FISC. *See* S. Rep. No. 111-92, at 24 (2009) (additional views from Senators Sessions, Hatch, Grassley, Kyl, Graham, Cornyn, and Coburn) (“It should be made clear that the changes to the business record and pen register statutes are intended to codify current practice under the relevance standard and are not intended to prohibit or restrict any activities approved by the FISA Court under existing authorities.”). This record is further evidence of awareness and approval by Members of Congress of the FISC’s decision that Section 215 authorizes the telephony metadata collection program.

Even if a subscriber subjectively intends to keep the numbers dialed secret, the Court held, “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44. The Court explained that someone who uses a phone has “voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business,” and therefore has “assumed the risk that the company would reveal to the police the numbers [] dialed.” *Id.* at 744.

Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in *Smith*, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes. Under longstanding Supreme Court precedent, this conclusion holds even if there is an understanding that the third party will treat the information as confidential. *See, e.g., SEC v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 743 (1984); *United States v. Miller*, 425 U.S. 435, 443 (1976) (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a *third* party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”) (emphasis added). Nothing in *United States v. Jones*, 132 S. Ct. 945 (2012), changed that understanding of the Fourth Amendment. The Court’s decision in that case concerned only whether physically attaching a GPS tracking device to an automobile to collect information was a Fourth Amendment search or seizure. The telephony metadata collection program does not involve tracking locations from which telephone calls are made, and does not involve physical trespass. *See United States v. Anderson-Bagshaw*, 2012 WL 774964, at \*2 (N.D. Ohio. Mar. 8, 2012) (“The [*Jones*] majority limited its analysis to the trespassory nature of the GPS installation, refusing to establish some point at which uninterrupted surveillance might become constitutionally problematic.”).

The scope of the program does not alter the conclusion that the collection of telephony metadata under a Section 215 court order is consistent with the Fourth Amendment. Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search. Further, Fourth Amendment rights “are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched.” *Steagald v. United States*, 451 U.S. 204, 219 (1981); *accord, e.g., Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (“Fourth Amendment rights are personal rights which . . . may not be vicariously asserted.”) (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Because the Fourth Amendment bestows “a personal right that must be invoked by an individual,” a person “claim[ing] the protection of the Fourth Amendment . . . must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable.” *Minnesota v. Carter*, 525 U.S. 83, 88 (1998). No Fourth Amendment-protected interest is generated by virtue of the fact that the telephony metadata records of many individuals are collected rather than those of a single individual. *Cf. In re Grand Jury Proceedings*, 827 F.2d at 305 (rejecting a money transfer business’ argument that a subpoena for records of all transfers made from a certain office was

unreasonable and overbroad under the Fourth Amendment because it “may make available to the grand jury records involving hundreds of innocent people”).

Even if one were to assume *arguendo* that the collection of telephony metadata involved a “search” within the meaning of the Fourth Amendment, for the reasons discussed above (*see* p. 15, *supra*), that search would satisfy the reasonableness standard that the Supreme Court has established in its cases authorizing the Government to conduct large-scale, but minimally intrusive, suspicionless searches. That standard requires a balancing of “the promotion of legitimate Governmental interests against the degree to which [the search] intrudes upon an individual’s privacy.” *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted). Such a balance of interests overwhelmingly favors the Government in this context. If any Fourth Amendment privacy interest were implicated by collection of telephony metadata, which does not include the content of any conversations, it would be minimal. Moreover, the intrusion on that interest would be substantially reduced by judicial orders providing that the data may be examined by an NSA analyst only when there is a “reasonable, articulable suspicion” that the seed identifier that is proposed for querying the data is associated with a specific foreign terrorist organization previously approved by the Court. Indeed, as the program has been conducted, only an exceedingly small fraction of the data collected has ever been seen—a fact that weighs heavily in the Fourth Amendment calculus. *See, e.g., id.* at 1979 (relying on safeguards that limited DNA analysis to identification information alone, without revealing any private information, as reducing any intrusion into privacy); *Vernonia School District 47J v. Acton*, 515 U.S. 646, 658 (1995) (finding it significant that urine testing of student athletes looked only for certain drugs, not for any medical conditions, as reducing any intrusion on privacy).

On the other side of the balance, there is an exceptionally strong public interest in the prevention of terrorist attacks, and telephony metadata analysis can be an important part of achieving that objective. This interest does not merely entail “ordinary crime-solving,” *King*, 133 S. Ct. at 1982 (Scalia, J., dissenting), but rather the forward-looking prevention of the loss of life, including potentially on a catastrophic scale. Given that exceedingly important objective, and the minimal, if any, Fourth Amendment intrusion that the program entails, the program would be constitutional even if the Fourth Amendment’s reasonableness standard applied.

## **B. First Amendment**

The telephony metadata collection is also consistent with the First Amendment. It merits emphasis again in this context that the program does not collect the content of any communications and that the data may be queried only when the Government has a reasonable, articulable suspicion that a particular number is associated with a specific foreign terrorist organization. Section 215, moreover, expressly prohibits the collection of records for an investigation that is being conducted solely on the basis of protected First Amendment activity, if the investigation is of a U.S. person. The FBI is also prohibited under applicable Attorney General guidelines from predicating an investigation solely on the basis of activity protected by the First Amendment. The Court-imposed rules that restrict the Government’s queries to those based on terrorist-associated seed identifiers and preclude indiscriminate use of the telephony

metadata substantially mitigate any First Amendment concerns arising from the breadth of the collection.

In any event, otherwise lawful investigative activities conducted in good faith—that is, not for the purpose of deterring or penalizing activity protected by the First Amendment—do not violate the First Amendment. *See, e.g., Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1051 (D.C. Cir. 1978) (First Amendment protects activities “*subject to the general and incidental burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves*” directed at First Amendment conduct) (emphasis added); *United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989) (“use of undercover informants to infiltrate an organization engag[ed] in protected first amendment activities” must be part of an investigation “conducted in good faith; i.e., not for the purpose of abridging first amendment freedoms”). The Government’s collection of telephony metadata in support of investigative efforts against specific foreign terrorist organizations are not aimed at curtailing any First Amendment activities, whether free speech or associational activities. Rather, the collection is in furtherance of the compelling national interest in identifying and tracking terrorist operatives and ultimately in thwarting terrorist attacks, particularly against the United States. It therefore satisfies any “good faith” requirement for purposes of the First Amendment. *See Reporters Comm.*, 593 F.2d at 1052 (“[T]he Government’s good faith inspection of defendant telephone companies’ toll call records does not infringe on plaintiffs’ First Amendment rights, because that Amendment guarantees no freedom from such investigation.”)

Nor does the Government’s collection and targeted analysis of metadata violate the First Amendment because of an asserted “chilling effect” on First Amendment-protected speech or association. The Supreme Court has held that an otherwise constitutionally reasonable search of international mail, though not based on probable cause or a warrant, does not impermissibly chill the exercise of First Amendment rights, at least where regulations preclude the Government from reading the content of any correspondence without a warrant. *See United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (noting that because envelopes are opened at the border only when customs officers have reason to suspect they contain something other than correspondence, and reading of correspondence is forbidden absent a warrant, any “chill” that might exist is both minimal and subjective and there is no infringement of First Amendment rights). Similarly, the bulk telephony metadata is queried only where there is a reasonable, articulable suspicion that the identifier used to query the data is associated with a particular foreign terrorist organization, and the program does not involve the collection of any content, let alone the review of such content.

The Executive Branch and the FISC have enacted strict oversight standards to guard against any potential for misuse of the data, and mandatory reporting to the FISC and Congress are designed to make certain that, when significant compliance problems are identified, they are promptly addressed with the active engagement of all three branches of Government. This system of checks and balances guarantees that the telephony metadata is not used to infringe First Amendment protected rights while also ensuring that it remains available to the Government to use for one of its most important responsibilities—protecting its people from international terrorism.



9 August 2013

## National Security Agency

---

### **The National Security Agency: Missions, Authorities, Oversight and Partnerships**

*“That’s why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse.”*

*--President Obama, May 23, 2013*

In his May 2013 address at the National Defense University, the President made clear that we, as a Government, need to review the surveillance authorities used by our law enforcement and intelligence community professionals so that we can collect information needed to keep us safe and ensure that we are undertaking the right kinds of privacy protections to prevent abuse. In the wake of recent unauthorized disclosures about some of our key intelligence collection programs, President Obama has directed that as much information as possible be made public, while mindful of the need to protect sources, methods and national security. Acting under that guidance, the Administration has provided enhanced transparency on, and engaged in robust public discussion about, key intelligence collection programs undertaken by the National Security Agency (NSA). This is important not only to foster the kind of debate the President has called for, but to correct inaccuracies that have appeared in the media and elsewhere. This document is a step in that process, and is aimed at providing a succinct description of NSA’s mission, authorities, oversight and partnerships.

### **Prologue**

After the al-Qa’ida attacks on the World Trade Center and the Pentagon, the 9/11 Commission found that the U.S. Government had failed to identify and connect the many “dots” of information that would have uncovered the planning and preparation for those attacks. We now know that 9/11 hijacker Khalid al-Midhar, who was on board American Airlines flight 77 that crashed into the Pentagon, resided in California for the first six months of 2000. While NSA had intercepted some of Midhar’s conversations with persons in an al-Qa’ida safe house in Yemen during that period, NSA did not have the U.S. phone number or any indication that the phone Midhar was using was located in San Diego. NSA did not have the tools or the database to search to identify these connections and share them with the FBI. Several programs were developed to address the U.S. Government’s need to connect the dots of information available to the intelligence community and to strengthen the coordination between foreign intelligence and domestic law enforcement agencies.



## **Background**

NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes. NSA performs this mission by engaging in the collection of “signals intelligence,” which, quite literally, is the production of foreign intelligence through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire, or other electromagnetic means. Every intelligence activity NSA undertakes is necessarily constrained to these central foreign intelligence and counterintelligence purposes. NSA’s challenge in an increasingly interconnected world -- a world where our adversaries make use of the same communications systems and services as Americans and our allies -- is to find and report on the communications of foreign intelligence value while respecting privacy and civil liberties. We do not need to sacrifice civil liberties for the sake of national security – both are integral to who we are as Americans. NSA can and will continue to conduct its operations in a manner that respects both. We strive to achieve this through a system that is carefully designed to be consistent with *Authorities* and *Controls* and enabled by capabilities that allow us to *Collect, Analyze, and Report* intelligence needed to protect national security.

## **NSA Mission**

NSA’s mission is to help protect national security by providing policy makers and military commanders with the intelligence information they need to do their jobs. NSA’s priorities are driven by externally developed and validated intelligence requirements, provided to NSA by the President, his national security team, and their staffs through the National Intelligence Priorities Framework.

## **NSA Collection Authorities**

NSA’s collection authorities stem from two key sources: Executive Order 12333 and the Foreign Intelligence Surveillance Act of 1978 (FISA).

### **Executive Order 12333**

Executive Order 12333 is the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. To the extent a person located outside the United States communicates with someone inside the United States or someone inside the United States communicates with a person located outside the United States those communications could also be collected. Collection pursuant to EO 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA. Intelligence activities conducted under this authority are carried out in accordance with minimization procedures established by the Secretary of Defense and approved by the Attorney General.

To undertake collections authorized by EO 12333, NSA uses a variety of methodologies. Regardless of the specific authority or collection source, NSA applies the process described below.

1. NSA identifies foreign entities (persons or organizations) that have information responsive to an identified foreign intelligence requirement. For instance, NSA works to identify individuals who may belong to a terrorist network.
2. NSA develops the “network” with which that person or organization’s information is shared or the command and control structure through which it flows. In other words, if NSA is tracking a specific terrorist, NSA will endeavor to determine who that person is in contact with, and who he is taking direction from.
3. NSA identifies how the foreign entities communicate (radio, e-mail, telephony, etc.)
4. NSA then identifies the telecommunications infrastructure used to transmit those communications.
5. NSA identifies vulnerabilities in the methods of communication used to transmit them.
6. NSA matches its collection to those vulnerabilities, or develops new capabilities to acquire communications of interest if needed.

This process will often involve the collection of communications metadata – data that helps NSA understand where to find valid foreign intelligence information needed to protect U.S. national security interests in a large and complicated global network. For instance, the collection of overseas communications metadata associated with telephone calls – such as the telephone numbers, and time and duration of calls – allows NSA to map communications between terrorists and their associates. This strategy helps ensure that NSA’s collection of communications content is more precisely focused on only those targets necessary to respond to identified foreign intelligence requirements.

NSA uses EO 12333 authority to collect foreign intelligence from communications systems around the world. Due to the fragility of these sources, providing any significant detail outside of classified channels is damaging to national security. Nonetheless, every type of collection undergoes a strict oversight and compliance process internal to NSA that is conducted by entities within NSA other than those responsible for the actual collection.

### **FISA Collection**

FISA regulates certain types of foreign intelligence collection including certain collection that occurs with compelled assistance from U.S. telecommunications companies. Given the techniques that NSA must employ when conducting NSA’s foreign intelligence mission, NSA quite properly relies on FISA authorizations to acquire significant foreign intelligence information and will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S. The FISA Court plays an important role in helping to ensure that signals intelligence collection governed by FISA is conducted in conformity with the requirements of the statute. All three branches of the U.S. Government have responsibilities for programs conducted under FISA, and a key role of the FISA Court is to ensure that activities conducted pursuant to FISA authorizations are consistent with the statute, as well as the U.S. Constitution, including the Fourth Amendment.

### **FISA Section 702**

Under Section 702 of the FISA, NSA is authorized to target non-U.S. persons who are reasonably believed to be located outside the United States. The principal application of this

authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States is a principal hub in the world's telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans. In general, Section 702 authorizes the Attorney General and Director of National Intelligence to make and submit to the FISA Court written certifications for the purpose of acquiring foreign intelligence information. Upon the issuance of an order by the FISA Court approving such a certification and the use of targeting and minimization procedures, the Attorney General and Director of National Intelligence may jointly authorize for up to one year the targeting of non-United States persons reasonably believed to be located overseas to acquire foreign intelligence information. The collection is acquired through compelled assistance from relevant electronic communications service providers.

NSA provides specific identifiers (for example, e-mail addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification. Once approved, those identifiers are used to select communications for acquisition. Service providers are compelled to assist NSA in acquiring the communications associated with those identifiers.

For a variety of reasons, including technical ones, the communications of U.S. persons are sometimes incidentally acquired in targeting the foreign entities. For example, a U.S. person might be courtesy copied on an e-mail to or from a legitimate foreign target, or a person in the U.S. might be in contact with a known terrorist target. In those cases, minimization procedures adopted by the Attorney General in consultation with the Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court are used to protect the privacy of the U.S. person. These minimization procedures control the acquisition, retention, and dissemination of any U.S. person information incidentally acquired during operations conducted pursuant to Section 702.

The collection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world. One notable example is the Najibullah Zazi case. In early September 2009, while monitoring the activities of al Qaeda terrorists in Pakistan, NSA noted contact from an individual in the U.S. that the FBI subsequently identified as Colorado-based Najibullah Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with al Qaeda, as well as identify any foreign or domestic terrorist links. The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi pled guilty to conspiring to bomb the New York City subway system. The FAA Section 702 collection against foreign terrorists was critical to the discovery and disruption of this threat to the U.S.

### **FISA (Title I)**

NSA relies on Title I of FISA to conduct electronic surveillance of foreign powers or their agents, to include members of international terrorist organizations. Except for certain narrow

exceptions specified in FISA, a specific court order from the Foreign Intelligence Surveillance Court based on a showing of probable cause is required for this type of collection.

### **Collection of U.S. Person Data**

There are three additional FISA authorities that NSA relies on, after gaining court approval, that involve the acquisition of communications, or information about communications, of U.S. persons for foreign intelligence purposes on which additional focus is appropriate. These are the Business Records FISA provision in Section 501 (also known by its section numbering within the PATRIOT Act as Section 215) and Sections 704 and 705(b) of the FISA.

#### **Business Records FISA, Section 215**

Under NSA's Business Records FISA program (or BR FISA), first approved by the Foreign Intelligence Surveillance Court (FISC) in 2006 and subsequently reauthorized during two different Administrations, four different Congresses, and by 14 federal judges, specified U.S. telecommunications providers are compelled by court order to provide NSA with information about telephone calls to, from, or within the U.S. The information is known as metadata, and consists of information such as the called and calling telephone numbers and the date, time, and duration of the call – but no user identification, content, or cell site locational data. The purpose of this particular collection is to identify the U.S. nexus of a foreign terrorist threat to the homeland

The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an “identifier,” such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a “seed.” Specifically, under Court-approved rules applicable to the program, there must be a “reasonable, articulable suspicion” that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. When the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. The “reasonable, articulable suspicion” requirement protects against the indiscriminate querying of the collected data. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

The BR FISA program is used in cases where there is believed to be a threat to the homeland. Of the 54 terrorism events recently discussed in public, 13 of them had a homeland nexus, and in 12 of those cases, BR FISA played a role. Every search into the BR FISA database is auditable and all three branches of our government exercise oversight over NSA's use of this authority.

#### **FISA Sections 704 and 705(b)**

FISA Section 704 authorizes the targeting of a U.S. person outside the U.S. for foreign intelligence purposes if there is probable cause to believe the U.S. person is a foreign power or is an officer, employee, or agent of a foreign power. This requires a specific, individual court order

by the Foreign Intelligence Surveillance Court. The collection must be conducted using techniques not otherwise regulated by FISA.

Section 705(b) permits the Attorney General to approve similar collection against a U.S. person who is already the subject of a FISA court order obtained pursuant to Section 105 or 304 of FISA. The probable cause standard has, in these cases, already been met through the FISA court order process.

### **Scope and Scale of NSA Collection**

According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that. However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission – that's less than one part in a million. Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.

### **The Essential Role of Corporate Communications Providers**

Under all FISA and FAA programs, the government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need. The government employs covernames to describe its collection by source. Some that have been revealed in the press recently include FAIRVIEW, BLARNEY, OAKSTAR, and LITHIUM. While some have tried to characterize the involvement of such providers as separate programs, that is not accurate. The role of providers compelled to provide assistance by the FISC is identified separately by the Government as a specific facet of the lawful collection activity.

### **The Essential Role of Foreign Partners**

NSA partners with well over 30 different nations in order to conduct its foreign intelligence mission. In every case, NSA does not and will not use a relationship with a foreign intelligence service to ask that service to do what NSA is itself prohibited by law from doing. These partnerships are an important part of the U.S. and allied defense against terrorists, cyber threat actors, and others who threaten our individual and collective security. Both parties to these relationships benefit.

One of the most successful sets of international partnerships for signals intelligence is the coalition that NSA developed to support U.S. and allied troops in Iraq and Afghanistan. The combined efforts of as many as 14 nations provided signals intelligence support that saved U.S. and allied lives by helping to identify and neutralize extremist threats across the breadth of both battlefields. The senior U.S. commander in Iraq credited signals intelligence with being a prime reason for the significant progress made by U.S. troops in the 2008 surge, directly enabling the removal of almost 4,000 insurgents from the battlefield.

## **The Oversight and Compliance Framework**

NSA has an internal oversight and compliance framework to provide assurance that NSA's activities – its people, its technology, and its operations – act consistently with the law and with NSA and U.S. intelligence community policies and procedures. This framework is overseen by multiple organizations external to NSA, including the Director of National Intelligence, the Attorney General, the Congress, and for activities regulated by FISA, the Foreign Intelligence Surveillance Court.

NSA has had different minimization procedures for different types of collection for decades. Among other things, NSA's minimization procedures, to include procedures implemented by United States Signals Intelligence Directive No. SP0018 (USSID 18), provide detailed instructions to NSA personnel on how to handle incidentally acquired U.S. person information. The minimization procedures reflect the reality that U.S. communications flow over the same communications channels that foreign intelligence targets use, and that foreign intelligence targets often discuss information concerning U.S. persons, such as U.S. persons who may be the intended victims of a planned terrorist attack. Minimization procedures direct NSA on the proper way to treat information at all stages of the foreign intelligence process in order to protect U.S. persons' privacy interests.

In 2009 NSA stood up a formal Director of Compliance position, affirmed by Congress in the FY2010 Intelligence Authorization Bill, which monitors verifiable consistency with laws and policies designed to protect U.S. person information during the conduct of NSA's mission. The program managed by the Director of Compliance builds on a number of previous efforts at NSA, and leverages best practices from the professional compliance community in industry and elsewhere in the government. Compliance at NSA is overseen internally by the NSA Inspector General and is also overseen by a number of organizations external to NSA, including the Department of Justice, the Office of the Director of National Intelligence, and the Assistant Secretary of Defense for Intelligence Oversight, the Congress, and the Foreign Intelligence Surveillance Court.

In addition to NSA's compliance safeguards, NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. This self-reporting is part of the culture and fabric of NSA. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to constantly improve.