

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*,

Plaintiffs,

v.

FEDERAL BUREAU OF INVESTIGATION, *et al.*,

Defendants.

11 Civ. 7562 (WHP)

ECF CASE

**DECLARATION OF CHARLES S. SIMS IN SUPPORT OF
PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF
CROSS-MOTION FOR SUMMARY JUDGMENT AND IN OPPOSITION
TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

I, Charles S. Sims, declare as follows:

1. I am a partner with Proskauer Rose, LLP, counsel for Plaintiffs in the above-referenced matter. I am familiar with and have personal knowledge of the facts set forth herein and could and would testify competently thereto if called upon to do so.
2. Attached hereto as Exhibit 1 is a copy of *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* (Aug. 9, 2013).
3. Attached hereto as Exhibit 2 is a copy of the April 25, 2013 Primary Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]* (FISC, No. BR 13-80).
4. Attached hereto as Exhibit 3 is a copy of Plaintiffs' May 31, 2011 Freedom of Information Act request.
5. Attached hereto as Exhibit 4 is a copy of the December 12, 2008 Supplemental Opinion, *In re Production of Tangible Things from [Redacted]* (FISC, No. BR 08-13).

6. Attached hereto as Exhibit 5 is a copy of the November 23, 2010 Supplemental Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]* (FISC, No. BR 10-82).

Dated: May 2, 2014
New York, NY



Charles S. Sims

Proskauer Rose LLP
11 Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900
csims@proskauer.com

**SIMS DECLARATION
EXHIBIT 1**

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,¹ 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).² 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

¹ "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).

² 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).³

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”).⁴ Moreover, a judge may grant an order for production of records under

³ 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).

⁴ 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)(H)(i). That further confirms that Section 215 applies to electronically stored information.⁵

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).

⁵ 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).⁶ 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*

⁶ 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.⁷ 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.⁸ 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.⁹ 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

⁷ *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).

⁸ *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").

⁹ *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.”)¹⁰ 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.¹¹

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.

¹⁰ 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”)

¹¹ 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.¹²

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

¹² 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." *Oklahoma Press Publishing 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.¹³

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 215.¹⁴ 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

¹³ 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)*.

¹⁴ *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 (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).¹⁵

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.

¹⁵ 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.

SIMS DECLARATION
EXHIBIT 2

~~TOP SECRET//SI//NOFORN~~

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D. C.

IN RE APPLICATION OF THE FEDERAL
BUREAU OF INVESTIGATION FOR AN
ORDER REQUIRING THE PRODUCTION
OF TANGIBLE THINGS FROM [REDACTED]

[REDACTED]

Docket Number: BR

13 - 8 0

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

~~TOP SECRET//SI//NOFORN~~

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought 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. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [REDACTED] and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"¹ created by [REDACTED]

B. The Custodian of Records of [REDACTED]
[REDACTED]
[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

¹ For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.² The BR metadata shall carry unique markings such

² The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.³

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms⁴ that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

³ The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [REDACTED], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.⁵ NSA shall ensure, through adequate and

⁵ For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.⁶

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED]

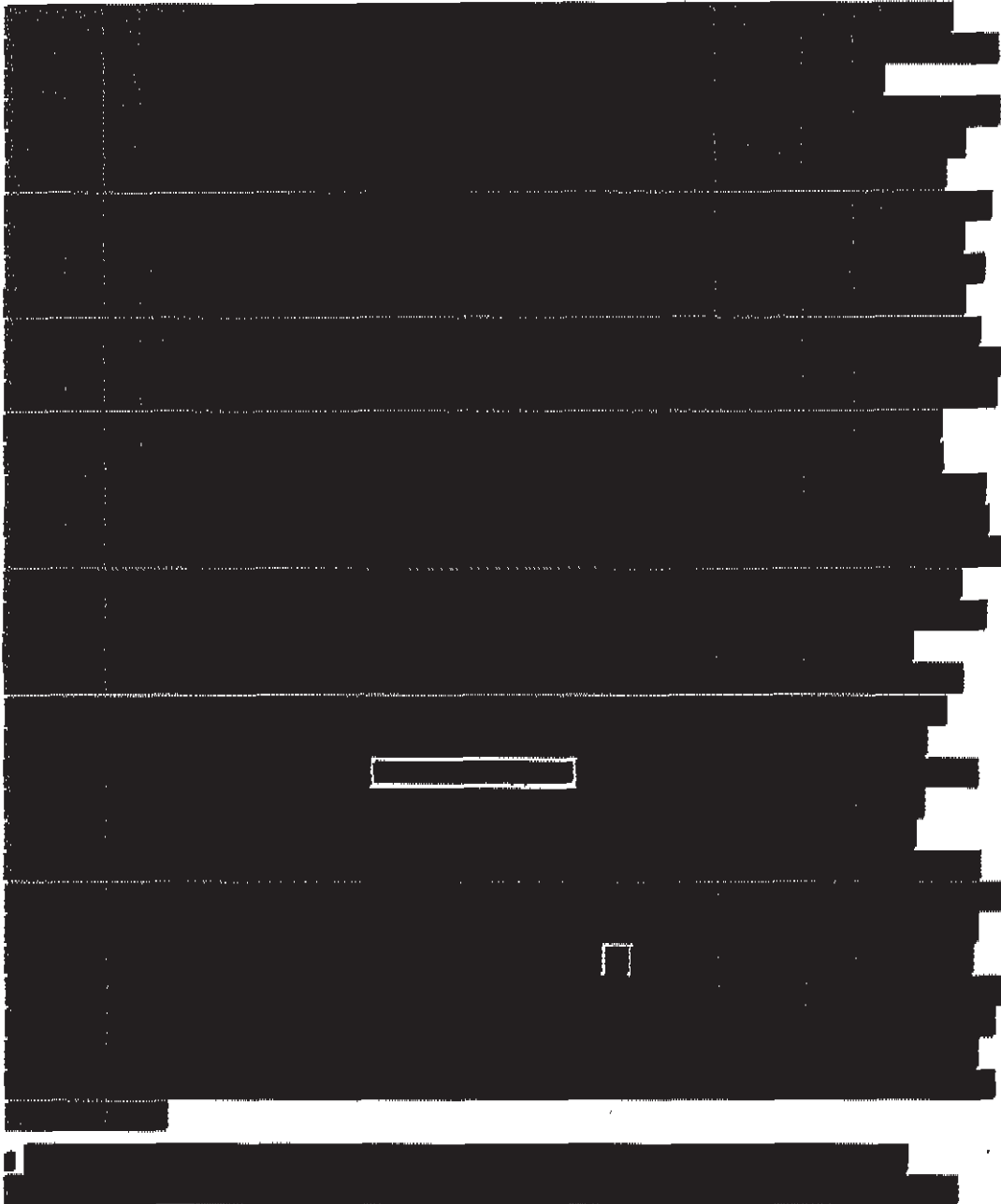
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

 provided, however, that NSA's Office of General Counsel (OGC)



~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [REDACTED] [REDACTED] [REDACTED] on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [REDACTED] [REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.^{9,10}

⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [REDACTED] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.¹¹ This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [REDACTED] Declaration, are as follows:

[REDACTED]

¹¹ This automated query process was initially approved by this Court in its [REDACTED] 2012 Order amending docket number [REDACTED].

¹² As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[REDACTED]

[REDACTED]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.¹⁵ NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.¹⁶ Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

¹⁵ In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

¹⁶ In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.¹⁷ OGC shall provide NSD/DoJ with copies

¹⁷ The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

counterterrorism information or to assess its importance.

This authorization regarding [REDACTED]

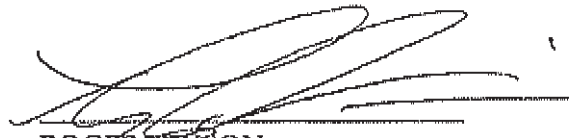
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] expires on the 19th day of July, 2013, at 5.00 p.m., Eastern Time.

Signed 04-25-2013 02:26 Eastern Time
Date Time

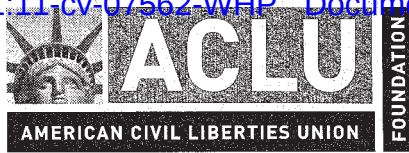


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

SIMS DECLARATION
EXHIBIT 3



FOIA/PA Mail Referral Unit
Department of Justice
LOC Building, Room 115
Washington, DC 20530-0001

Carmen L. Mallon
Chief of Staff
Office of Information Policy
Department of Justice
Attn: FOI/PA Request
1425 New York Avenue, N.W., Suite 11050
Washington, D.C. 20530-0001

Office of Public Affairs
Department of Justice
950 Pennsylvania Avenue, NW., Room 1128
Washington DC 20530-0001

Federal Bureau of Investigation
Record/Information Dissemination Section
Attn: FOI/PA Request
170 Marcel Drive
Winchester, VA 22602-4843

Elizabeth Farris,
Supervisory Paralegal
Office of Legal Counsel
Department of Justice
Attn: FOI/PA Request
950 Pennsylvania Avenue, NW, Room 5515
Washington, DC 20530-0001

National Security Division
U.S. Department of Justice
Attn: FOI/PA Request
950 Pennsylvania Avenue, N.W., Room 6150
Washington, D.C. 20530-0001

**AMERICAN CIVIL LIBERTIES
UNION FOUNDATION**

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS

SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

RICHARD ZACKS
TREASURER

May 31, 2011

Dear Freedom of Information Officer,

This letter constitutes a request under the Freedom of Information Act, 5 U.S.C. § 552 (“FOIA”). It is submitted on behalf of the American Civil Liberties Union and the American Civil Liberties Foundation (together, the “ACLU”).¹

I. Background

This request pertains to the use by the Federal Bureau of Investigation (“FBI”) of the powers enumerated in Pub. L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, commonly known as the USA PATRIOT Act (“PATRIOT Act”). Specifically, this request pertains to the FBI’s use and interpretation of Section 215 of the PATRIOT Act, as amended, which permits the government to apply for court orders requiring the production of “tangible things.”

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

II. Records Requested

We request that you release to us any and all records concerning the government’s interpretation or use of Section 215, including but not limited to: legal opinions or memoranda interpreting that provision; guidelines informing government personnel how that provision can be used; records containing statistics about the use or misuse of the provision; reports provided by the executive branch to Congress relating to the executive’s interpretation, use, or misuse of the provision; forms used by executive agencies in connection with the use of Section 215; and legal papers filed by the government or any other party in the Foreign Intelligence Surveillance Court, and opinions of that court, pertaining to the interpretation, use, or proposed use of Section 215.

With respect to the records described above, we seek only those records drafted, finalized, or issued after March 9, 2006. We do not ask you to disclose the names or identities of those entities or individuals

¹ The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analyses of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

who have been served with Section 215 orders or the names or identities of those individuals or entities about whom records have been sought, but we ask that you disclose any and all records indicating the kinds or types of information that may, as a matter of policy or law, be obtained through the use of Section 215.

With respect to the form of production, *see* 5 U.S.C. § 552(a)(3)(B), we request that responsive electronic records be provided electronically in their native file format, if possible. Alternatively, we request that the records be provided electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and that the records be provided in separate, bates-stamped files.

If any aspect of our request is unclear, we would welcome the opportunity to clarify it. We would also welcome the opportunity to discuss an appropriate processing schedule.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

III. Application for Expedited Processing

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E); 28 C.F.R. § 16.5(d). Expedited processing is warranted because the records sought are urgently needed by an organization primarily engaged in disseminating information in order to inform the public about actual or alleged federal government activity, 28 C.F.R. § 16.5(d)(1)(ii), and because the records sought relate to a "matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence," *id.* § 16.5(d)(1)(iv).

A. Expedited processing is warranted under 28 C.F.R. § 16.5(d)(ii)

The records requested are needed to inform the public about federal government activity. The records relate to the FBI's use of a highly controversial surveillance authority. Specifically, the records requested relate to the FBI's use of Section 215 and to the process the FBI has put in place to ensure that the FBI's use of Section 215 powers conforms to the requirements of the Constitution and statutory law. The records are urgently needed because of recent allegations by some members of the Senate Select Committee on Intelligence that the Justice Department has adopted an overly broad interpretation of Section 215,²

² *See* Charlie Savage, *Senators Say Patriot Act Is Being Misinterpreted*, N.Y. Times, May 26, 2011, available at <http://www.nytimes.com/2011/05/27/us/27patriot.html>; Spencer Ackerman, *There's a Secret Patriot Act, Senator Says*, Wired.com, May 25, 2011, available at <http://www.wired.com/dangerroom/2011/05/secret-patriot-act/>; 157

and because there is an ongoing debate about the appropriate scope of the government's surveillance authorities.³

The ACLU is "primarily engaged in disseminating information" within the meaning of the statute and regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(d)(1)(ii). Disseminating information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public is a critical and substantial component of the ACLU's work and one of its primary activities. See *ACLU v. Dep't of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding non-profit public interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience" to be "primarily engaged in disseminating information" (internal citation omitted)).

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Cong. Rec. S3259-60 (daily ed. May 24, 2011), available at <http://www.gpo.gov/fdsys/pkg/CREC-2011-05-24/pdf/CREC-2011-05-24-pt1-PgS3247-7.pdf#page=1>.

³ See, e.g., *Obama signs Patriot Act extension; will continue anti-terror surveillance powers*, Assoc. Press, May 25, 2011, available at http://www.washingtonpost.com/politics/senate-moves-patriot-act-toward-4-year-extension-before-thursday-midnight-deadline/2011/05/25/AGnYjXBH_story.html; *New tea party senator gets Senate's attention*, Assoc. Press, May 25, 2011, ("[Sen. Rand] Paul has delayed action on the intelligence-gathering measures, contending they should expire because the Patriot Act gives the government too much power to monitor people's lives."), available at <http://www.foxnews.com/us/2011/05/25/new-tea-party-senator-gets-senates-attention/>; Editorial, *A chance to put protections in the Patriot Act*, Wash. Post, May 25, 2011, available at http://www.washingtonpost.com/opinions/a-chance-to-put-protections-in-the-patriot-act/2011/05/25/AGsSPXBH_story.html; Felicia Sonmez, *Vote on Patriot Act extension delayed as Rand Paul pushes for amendment on gun rights*, Wash. Post, May 25, 2011, available at http://www.washingtonpost.com/blogs/2chambers/post/vote-on-patriot-act-extension-delayed-as-rand-paul-pushes-for-amendment-on-gun-rights/2011/05/25/AGhzDJBH_blog.html; David Kravets, *Lawmakers Punt Again on Patriot Act Reform*, Wired.com, May 20, 2011, available at <http://www.wired.com/threatlevel/2011/05/patriot-act-reform/>; David Kravets, *House Fails to Extend Patriot Act Spy Powers*, Kristy Sidor, *The Patriot Act Expiration Controversy*, The Observer at Boston College, Feb. 22, 2011, available at <http://www.thebcoobserver.com/2011/02/22/the-patriot-act-expiration-controversy/>; Wired.com, Feb. 8, 2011, available at <http://www.wired.com/threatlevel/2011/02/patriot-act-notextended/>; Charlie Savage, *Battle Looms Over the Patriot Act*, N.Y. Times, Sept. 19, 2009, available at <http://www.nytimes.com/2009/09/20/us/politics/20patriot.html?partner=rss&emc=rss>; Julian Sanchez, *A Chance to Fix the PATRIOT Act?* Cato At Liberty, Sept. 17, 2009, available at <http://www.cato-at-liberty.org/a-chance-to-fix-the-patriot-act/>; David Kravets, *Obama Backs Extending Patriot Act Spy Provisions*, Wired, Sept. 15, 2009, available at <http://www.wired.com/threatlevel/2009/09/obama-backs-expiring-patriot-act-spy-provisions/>; Adam Cohen, *Democratic Pressure on Obama to Restore the Rule of Law*, N.Y. Times, Nov. 18, 2008, available at <http://www.nytimes.com/2008/11/14/opinion/14fri4.html>.

The ACLU publishes newsletters, news briefings, right-to-know handbooks, and other materials that are disseminated to the public. Its material is available to everyone, including tax-exempt organizations, not-for-profit groups, law students, and faculty, for no cost or for a nominal fee. Since 2007, ACLU national projects have published and disseminated over 30 reports. Many ACLU reports include description and analysis of government documents obtained through FOIA.⁴

The ACLU also disseminates information through its website, www.aclu.org. The website addresses civil liberties issues in depth, provides features on civil liberties issues in the news, and contains hundreds of documents that relate to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, the ACLU also provides the public with educational material about the particular civil liberties issue or problem; recent news about the issue; analyses of Congressional or executive branch action on the issue; government documents obtained through FOIA about the issue; and more in-depth analytic and educational multi-media features on the issue.⁵ The ACLU website includes many features on information obtained through the FOIA.⁶ For example, the ACLU's "Torture

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

⁴ See, e.g., ACLU, Reclaiming Patriotism: A Call to Reconsider the Patriot Act (March 2009), available at http://www.aclu.org/pdfs/safe/free/patriot_report_20090310.pdf; ACLU, The Excluded: Ideological Exclusion and the War on Ideas (Oct. 2007), available at <http://www.aclu.org/national-security/excluded-ideological-exclusion-and-war-ideas>; ACLU, History Repeated: The Dangers of Domestic Spying by Federal Law Enforcement (May 2007), available at <http://www.aclu.org/files/FilesPDFs/mlkreport.pdf>; ACLU, No Real Threat: The Pentagon's Secret Database on Peaceful Protest (Jan. 2007), available at <http://www.aclu.org/national-security/no-real-threat-pentagons-secret-database-peaceful-protest>; ACLU, Unpatriotic Acts: The FBI's Power to Rifle Through Your Records and Personal Belongings Without Telling You (July 2003), available at http://www.aclu.org/files/FilesPDFs/spies_report.pdf.

⁵ For example, the ACLU's website about national security letter ("NSL") cases, www.aclu.org/nsl, includes, among other things, an explanation of what NSLs are; information about and document repositories for the ACLU's NSL cases; links to documents obtained through FOIA about various agencies' use of NSLs; NSL news in the courts, Congress, and executive agencies; links to original blog posts commenting on and analyzing NSL-related news; educational web features about the NSL gag power; public education reports about NSLs and the Patriot Act; news about and analysis of the Department of Justice Inspector General's reviews of the FBI's use of NSLs; the ACLU's policy analysis and recommendations for reform of the NSL power; charts with analyzed data about the government's use of NSLs; myths and facts documents; and links to information and analysis of related issues.

⁶ See, e.g., <http://www.aclu.org/accountability/released.html> (Torture FOIA); <http://www.aclu.org/accountability/olc.html> (OLC Memos);

FOIA” webpage, <http://www.aclu.org/accountability/released.html>, contains commentary about the ACLU’s FOIA request, press releases, analysis of the FOIA documents, and an advanced search engine permitting webpage visitors to search approximately 150,000 pages of documents obtained through the FOIA.

The ACLU has also published a number of charts that collect, summarize, and analyze information it has obtained through FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA—the ACLU has created a chart that provides the public and news media with a comprehensive index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition and surveillance and that describes what is publicly known about the memos and their conclusions, who authored them and for whom, and whether the memos remain secret or have been released to the public in whole or in part.⁷ Similarly, the ACLU produced a chart of original statistics about the Defense Department’s use of National Security Letters based on its own analysis of records obtained through FOIA.⁸

B. Expedited processing is warranted under 28 C.F.R. § 16.5(d)(iv)

The records requested also relate to a “matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence.” 28 C.F.R. § 16.5(d)(1)(iv).

Since the PATRIOT Act’s enactment in 2001, Section 215 has been the subject of considerable and sustained media attention.⁹ Over the

<http://www.aclu.org/national-security/csrt-foia> (CSRT FOIA); <http://www.aclu.org/national-security/aclu-v-doj-lawsuit-enforce-nsawarrantless-surveillance-foia-request> (NSA FOIA); <http://www.aclu.org/national-security/patriot-foia> (Patriot Act FOIA); <http://www.aclu.org/national-security-technology-and-liberty/spyfiles> (Spy Files).

⁷ The chart is available at http://www.aclu.org/files/assets/olcmemos_chart.pdf.

⁸ The chart is available at http://www.aclu.org/files/assets/nsl_stats.pdf.

⁹ See, e.g., Editorial, *Breaking a Promise on Surveillance*, N.Y. Times, July 29, 2010, available at <http://www.nytimes.com/2010/07/30/opinion/30fri1.html>; Editorial, *Patriot Act Excesses*, N.Y. Times, Oct. 7, 2009, available at <http://www.nytimes.com/2009/10/08/opinion/08thu1.html>; Press Release, Leahy renews effort to extend expiring PATRIOT Act provisions, available at <http://vtdigger.org/2011/01/27/leahy-renews-effort-to-extend-expiring-patriot-act-provisions/>; Fred H. Kate, Legal Restrictions on Transborder Data Flows to Prevent Government Access to Personal Data: Lessons from British Columbia, The Ctr. for Info. and Policy Leadership, Aug. 2005, available at

last months, as Congress has debated reauthorization of certain PATRIOT Act provisions, including Section 215, media and public attention has intensified.¹⁰ Many recent news stories have included allegations by members of the Senate Select Committee on Intelligence that the Department of Justice has adopted an overbroad construction of Section 215.¹¹ While the Department of Justice claimed only to have

<http://blog.surveymonkey.com/wp-content/uploads/2011/05/various-Canadians-have-made-similar-points.pdf>; Taking Issue: The Patriot Act: Section 215, NPR.org, July 21, 2005, available at http://www.npr.org/takingissue/20050721_takingissue_patriotact.html; Heather McDonald, *Patriot Act: Let Investigators Do Their Job*, NPR.org, July 20, 2005, available at <http://www.npr.org/templates/story/story.php?storyId=4763326>; Larry Abramson and Maria Godoy, *The Patriot Act: Key Controversies*, NPR, Dec. 16, 2005, available at <http://www.npr.org/news/specials/patriotact/patriotactdeal.html>; Dahlia Lithwick and Julia Turner, *A Guide to the Patriot Act, Part 1*, Slate, Sept. 8, 2003, available at <http://www.slate.com/id/2087984/>.

¹⁰ See, e.g., Charlie Savage, *Patriot Battle Could Hinder Investigators*, N.Y. Times, May 25, 2011, available at <http://www.nytimes.com/2011/05/26/us/politics/26patriot.html>; *Senate moves to break impasse, vote on controversial provision of Patriot Act*, Assoc. Press, May 24, 2011, available at http://www.washingtonpost.com/politics/congress-races-to-extend-patriot-act-send-to-obama-in-europe-before-friday-deadline/2011/05/24/AFrxmIAH_story.html; Charlie Savage, *Deal Reached on Extension of Patriot Act*, N.Y. Times, May 19, 2011, available at <http://www.nytimes.com/2011/05/20/us/20patriot.html>; Editorial, *In Patriot Act vote, Tea Party stands up for civil liberties*, Boston Globe, Feb. 14, 2011, available at http://www.boston.com/bostonglobe/editorial_opinion/editorials/articles/2011/02/14/in_patriot_act_vote_tea_party_stands_up_for_civil_liberties/; Tom Gantert, *Civil Liberties Concerns Caused Amash to Vote Against PATRIOT Act*, Michigan Capitol Confidential, Feb. 11, 2011, available at <http://www.michiganconfidential.com/14549>; Charlie Savage, *Battle Looms Over the Patriot Act*, *supra* note 3.

¹¹ See, e.g., *4 senators win promise of a Patriot Act hearing*, Assoc. Press, May 26, 2011, available at http://www.boston.com/news/nation/washington/articles/2011/05/26/2_senators_win_promise_of_patriot_act_hearings/; Spencer Ackerman, *There's a Secret Patriot Act, Senator Says*, Wired.com, see *supra* note 2; "Secret" legal interpretation of Patriot Act provisions troubles 4 Senators, Assoc. Press, May 26, 2011, available at http://www.washingtonpost.com/politics/secret-legal-interpretation-of-patriot-act-provisions-troubles-2-senators/2011/05/26/AGFczGCH_story.html; "Secret" legal interpretation of Patriot Act provisions troubles 2 Senators, Assoc. Press, May 26, 2011, available at http://www.washingtonpost.com/politics/secret-legal-interpretation-of-patriot-act-provisions-troubles-2-senators/2011/05/26/AG7ffICH_story.html; Charlie Savage, *Senators Say Patriot Act Is Being Misinterpreted*, N.Y. Times, May 26, 2011, see *supra*, note 2; Steven Aftergood, *Sen. Wyden Decries "Secret Law" on PATRIOT Act*, Secrecy News, May 25, 2011, available at http://www.fas.org/blog/secrecy/2011/05/wyden_secret_law.html; Marcy Wheeler, *Wyden and Udall Want Obama to Admit to Secret Collection Program*, Emptywheel, May 24, 2011, available at <http://emptywheel.firedoglake.com/2011/05/24/wyden-and-udall-want-obama-to-admit-to-secret-collection-program/>.

used Section 215 powers 21 times in 2009¹² and 96 times in 2010,¹³ Senators Ron Wyden and Mark Udall, along with others, recently proffered an amendment to address the government's "secret[] reinterpretation [of] public laws and statutes in a manner that is inconsistent with the public's understanding of these laws."¹⁴ In that same congressional session, Senator Ron Wyden stated in open Congress that he "certainly believe[s] the public will be surprised again when they learn about some of the interpretations of the PATRIOT Act," suggesting that the FBI's numbers or public statements may be misleading or incomplete.¹⁵

IV. Application for Waiver or Limitation of Fees

A. A waiver of search, review, and duplication fees is warranted under 28 C.F.R. § 16.11(k)(1).

The ACLU is entitled to a waiver of search, review, and duplication fees because disclosure of the requested records is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester. 5 U.S.C. § 552(a)(4)(A)(iii); 28 C.F.R. § 16.11(k)(1).

The requesters are making this request specifically to further the public's understanding of the government's use of surveillance powers inside the United States. As the dozens of new articles cited above make clear, disclosure of the requested records will contribute significantly to public understanding of the operations and activities of the government. *See* 28 C.F.R. § 16.11(k)(1)(i). Disclosure is not in the ACLU's commercial interest. Any information disclosed by the government in response to this FOIA request will be made available to the public at no

¹² *See* Letter to the Hon. Joseph R. Biden, Jr., Department of Justice, Office of Legislative Affairs, Apr. 30, 2011, *available at* <http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf>.

¹³ *See* Letter to the Hon. Harry Reid, Department of Justice, Office of Legislative Affairs, Apr. 29, 2011, *available at* <http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf>.

¹⁴ *See* 157 Cong. Rec. S3283 (daily ed. May 24, 2011) (SA 339, amendment of Mr. Wyden), *available at* <http://www.gpo.gov/fdsys/pkg/CREC-2011-05-24/pdf/CREC-2011-05-24-pt1-PgS3281.pdf#page=3>

¹⁵ *See* 157 Cong. Rec. S3258-62, (daily ed. May 24, 2011), *available at* <http://www.gpo.gov/fdsys/pkg/CREC-2011-05-24/pdf/CREC-2011-05-24-pt1-PgS3247-7.pdf#page=1>.

cost. A fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requests.'" (citation omitted)); OPEN Government Act of 2007, Pub. L. No. 110-175, § 2, 121 Stat. 2524 (Dec. 31, 2007) (finding that "disclosure, not secrecy, is the dominant objective of the Act," but that "in practice, the Freedom of Information Act has not always lived up to the ideals of the Act").

B. A waiver of search and review fees is warranted under 5 U.S.C. § 551(a)(4)(A)(ii) and 28 C.F.R. 16.11(c)(1)-(3), (d)(1).

A waiver of search and review fees is warranted because the ACLU qualifies as a "representative of the news media" and the records are not sought for commercial use. 5 U.S.C. § 551(a)(4)(A)(ii); 28 C.F.R. §§ 16.11(c)(1)-(3), (d)(1). The ACLU is a representative of the news media in that it is an organization "actively gathering news for an entity that is organized and operated to publish or broadcast news to the public," where "news" is defined as "information that is about current events or that would be of current interest to the public." 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.11(b)(6). Accordingly, fees associated with the processing of the Request should be "limited to reasonable standard charges for document duplication." 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.11 (d) (search and review fees shall not be charged to "representatives of the news media"); *id.* § 16.11(c)(3) (review fees charged only for "commercial use request[s]").

The ACLU meets the statutory and regulatory definitions of a "representative of the news media" because it "uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii); *see also Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that "gathers information from a variety of sources," exercises editorial discretion in selecting and organizing documents, "devises indices and finding aids," and "distributes the resulting work to the public" is a "representative of the news media" for purposes of FOIA); *cf. ACLU v. Dep't of Justice*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be "primarily engaged in disseminating information"). The ACLU is a "representative of the news media" for the same reasons it is "primarily engaged in the dissemination of information." *See e.g., Elec. Privacy Info. Ctr. v. Dep't of Def.*, 241 F. Supp. 2d 5, 10-15 (D.D.C. 2003) (finding nonprofit public interest group that disseminated an electronic newsletter and

published books was a “representative of the media” for purposes of FOIA).¹⁶

If the request is denied in whole or in part, we ask that you justify all withholdings by reference to specific exemptions to the FOIA. We also ask that you release all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information or to deny a waiver of fees.

Please be advised that, because we are requesting expedited processing under 28 C.F.R. §§ 16.11(d)(1)(iv) as well as 16.11(d)(1)(ii), we are sending a copy of this letter to DOJ’s Office of Public Affairs. Whatever the determination of that office, we look forward to your reply within 20 business days, as the statute requires under section 552(a)(6)(A)(I).

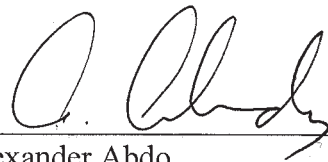
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Thank you for your prompt attention to this matter. Please furnish all applicable records to:

Jameel Jaffer
Deputy Legal Director
American Civil Liberties Union
125 Broad St., 18th Floor
New York, NY 10004

¹⁶ On account of these factors, fees associated with responding to FOIA requests are regularly waived on the grounds that the ACLU is a “representative of the news media.” In October 2010, the Department of the Navy granted a fee waiver to the ACLU with respect to a request for documents regarding the deaths of detainees in U.S. custody. In January 2009, the CIA granted a fee waiver with respect to the same request. In March 2009, the Department of State granted a fee waiver to the ACLU with respect to its request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists. Likewise, in December 2008, the Department of Justice granted the ACLU a fee waiver with respect to the same request. In May 2005, the Department of Commerce granted a fee waiver to the ACLU with respect to its request for information regarding the radio frequency identification chips in United States passports. In March 2005, the Department of State granted a fee waiver to the ACLU with respect to a request regarding the use of immigration laws to exclude prominent non-citizen scholars and intellectuals from the country because of their political views. Also, the Department of Health and Human Services granted a fee waiver to the ACLU with regard to a FOIA request submitted in August of 2004. In addition, the Office of Science and Technology Policy in the Executive Office of the President said it would waive the fees associated with a FOIA request submitted by the ACLU in August 2003. Finally, three separate agencies—the Federal Bureau of Investigation, the Office of Intelligence Policy and Review, and the Office of Information and Privacy in the Department of Justice—did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

Under penalty of perjury, I hereby affirm that the foregoing is true and correct to the best of my knowledge and belief.



Alexander Abdo
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel. 212-519-7814
Fax 212-549-2654

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

SIMS DECLARATION
EXHIBIT 4

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE PRODUCTION OF TANGIBLE THINGS FROM :

[REDACTED]

Docket No.: BR 08-13

SUPPLEMENTAL OPINION

This Supplemental Opinion memorializes the Court’s reasons for concluding that the records to be produced pursuant to the orders issued in the above-referenced docket number are properly subject to production pursuant to 50 U.S.C.A. § 1861 (West 2003 & Supp. 2008), notwithstanding the provisions of 18 U.S.C.A. §§ 2702-2703 (West 2000 & Supp. 2008), amended by Public Law 110-401, § 501(b)(2) (2008).

As requested in the application, the Court is ordering production of telephone “call detail records or ‘telephony metadata,’” which “includes comprehensive communications routing information, including but not limited to session identifying information . . . , trunk identifier, telephone calling card numbers, and time and duration of [the] calls,” but “does not include the substantive content of any communication.” Application at 9; Primary Order at 2. Similar productions have been ordered by judges of the Foreign Intelligence Surveillance Court (“FISC”). See Application at 17. However, this is the first application in which the government has identified the provisions of 18 U.S.C.A. §§ 2702-2703 as potentially relevant to whether such orders could properly be issued under 50 U.S.C.A. § 1861. See Application at 6-8.

Pursuant to section 1861, the government may apply to the FISC “for an order requiring the production of any tangible things (including books, records, papers, documents, and other items).” 50 U.S.C.A. § 1861(a)(1) (emphasis added). The FISC is authorized to issue the order, “as requested, or as modified,” upon a finding that the application meets the requirements of that section. Id. at § 1861(c)(1). Under the rules of statutory construction, the use of the word “any” in a statute naturally connotes “an expansive meaning,” extending to all members of a common set, unless Congress employed “language limiting [its] breadth.” United States v. Gonzales, 520 U.S. 1, 5 (1997); accord Ali v. Federal Bureau of Prisons, 128 S. Ct. 831, 836 (2008)

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

(“Congress’ use of ‘any’ to modify ‘other law enforcement officer’ is most naturally read to mean law enforcement officers of whatever kind.”).¹

However, section 2702, by its terms, describes an apparently exhaustive set of circumstances under which a telephone service provider may provide to the government non-content records pertaining to a customer or subscriber. See § 2702(a)(3) (except as provided in § 2702(c), a provider “shall not knowingly divulge a record or other [non-content] information pertaining to a subscriber or customer . . . to any governmental entity”). In complementary fashion, section 2703 describes an apparently exhaustive set of means by which the government may compel a provider to produce such records. See § 2703(c)(1) (“A governmental entity may require a provider . . . to disclose a record or other [non-content] information pertaining to a subscriber . . . or customer . . . only when the governmental entity” proceeds in one of the ways described in § 2703(c)(1)(A)-(E)) (emphasis added). Production of records pursuant to a FISC order under section 1861 is not expressly contemplated by either section 2702(c) or section 2703(c)(1)(A)-(E).

If the above-described statutory provisions are to be reconciled, they cannot all be given their full, literal effect. If section 1861 can be used to compel production of call detail records, then the prohibitions of section 2702 and 2703 must be understood to have an implicit exception for production in response to a section 1861 order. On the other hand, if sections 2702 and 2703 are understood to prohibit the use of section 1861 to compel production of call detail records, then the expansive description of tangible things obtainable under section 1861(a)(1) must be construed to exclude such records.

The apparent tension between these provisions stems from amendments enacted by Congress in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA PATRIOT Act”), Public Law 107-56, October 26, 2001, 115 Stat. 272. Prior to the USA PATRIOT Act, only limited types of records, not

¹ The only express limitation on the type of tangible thing that can be subject to a section 1861 order is that the tangible thing “can 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.” *Id.* at § 1861(c)(2)(D). Call detail records satisfy this requirement, since they may be obtained by (among other means) a “court order for disclosure” under 18 U.S.C.A. § 2703(d). Section 2703(d) permits the government to obtain a court order for release of non-content records, or even in some cases of the contents of a communication, upon a demonstration of relevance to a criminal investigation.

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

including call detail records, were subject to production pursuant to FISC orders.² Section 215 of the USA PATRIOT Act replaced this prior language with the broad description of “any tangible thing” now codified at section 1861(a)(1). At the same time, the USA PATRIOT Act amended sections 2702 and 2703 in ways that seemingly re-affirmed that communications service providers could divulge records to the government only in specified circumstances,³ without expressly referencing FISC orders issued under section 1861.

The government argues that section 1861(a)(3) supports its contention that section 1861(a)(1) encompasses the records sought in this case. Under section 1861(a)(3), which Congress enacted in 2006,⁴ applications to the FISC for production of several categories of sensitive records, including “tax return records” and “educational records,” may be made only by the Director, the Deputy Director or the Executive Assistant Director for National Security of the Federal Bureau of Investigation (“FBI”). 18 U.S.C.A. § 1861(a)(3). The disclosure of tax return records⁵ and educational records⁶ is specifically regulated by other federal statutes, which do not by their own terms contemplate production pursuant to a section 1861 order. Nonetheless, Congress clearly intended that such records could be obtained under a section 1861 order, as demonstrated by their inclusion in section 1861(a)(3). But, since the records of telephone service providers are not mentioned in section 1861(a)(3), this line of reasoning is not directly on point. However, it does at least demonstrate that Congress may have intended the sweeping description of tangible items obtainable under section 1861 to encompass the records of telephone service providers, even though the specific provisions of sections 2702 and 2703 were not amended in order to make that intent unmistakably clear.

² See 50 U.S.C.A. § 1862(a) (West 2000) (applying to records of transportation carriers, storage facilities, vehicle rental facilities, and public accommodation facilities).

³ Specifically, the USA PATRIOT Act inserted the prohibition on disclosure to governmental entities now codified at 18 U.S.C.A. § 2702(a)(3), and exceptions to this prohibition now codified at 18 U.S.C.A. § 2702(c). See USA PATRIOT Act § 212(a)(1)(B)(iii) & (E). The USA PATRIOT Act also amended the text of 18 U.S.C.A. § 2703(c)(1) to state that the government may require the disclosure of such records only in circumstances specified therein. See USA PATRIOT Act § 212(b)(1)(C)(i).

⁴ See Public Law 109-177 § 106(a)(2) (2006).

⁵ See 26 U.S.C.A. § 6103(a) (West Supp. 2008), amended by Public Law 110-328 § 3(b)(1) (2008).

⁶ See 20 U.S.C.A. § 1232g(b) (West 2000 & Supp. 2008).

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

The Court finds more instructive a separate provision of the USA PATRIOT Act, which also pertains to governmental access to non-content records from communications service providers. Section 505(a) of the USA PATRIOT Act amended provisions, codified at 18 U.S.C.A. § 2709 (West 2000 & Supp. 2008), enabling the FBI, without prior judicial review, to compel a telephone service provider to produce “subscriber information and toll billing records information.” 18 U.S.C.A. § 2709(a).⁷ Most pertinently, section 505(a)(3)(B) of the USA PATRIOT Act lowered the predicate required for obtaining such information to a certification submitted by designated FBI officials asserting its relevance to an authorized foreign intelligence investigation.⁸

Indisputably, section 2709 provides a means for the government to obtain non-content information in a manner consistent with the text of sections 2702-2703.⁹ Yet section 2709 merely requires an FBI official to provide a certification of relevance. In comparison, section 1861 requires the government to provide to the FISC a “statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant” to a foreign intelligence investigation,¹⁰ and the FISC to determine that the application satisfies this

⁷ This process involves service of a type of administrative subpoena, commonly known as a “national security letter.” David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 19:2 (2007).

⁸ Specifically, a designated FBI official must certify that the information or records sought are “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 18 U.S.C.A. § 2709(b)(1)-(2) (West Supp. 2008). Prior to the USA PATRIOT Act, the required predicate for obtaining “local and long distance toll billing records of a person or entity” was “specific and articulable facts giving reason to believe that the person or entity . . . is a foreign power or an agent of a foreign power.” See 18 U.S.C.A. § 2709(b)(1)(B) (West 2000).

⁹ Section 2703(c)(2) permits the government to use “an administrative subpoena” to obtain certain categories of non-content information from a provider, and section 2709 concerns use of an administrative subpoena. See note 7 supra.

¹⁰ 50 U.S.C.A. § 1861(b)(2)(A). More precisely, the investigation must be “an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities,” id., “provided that such investigation of a United States
(continued...)

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

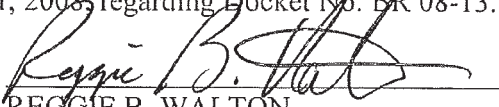
~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

requirement, see 50 U.S.C.A. § 1861(c)(1), before records are ordered produced. It would have been anomalous for Congress, in enacting the USA PATRIOT Act, to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to sections 2702-2703, but to have deemed the FISC's application of a closely similar "relevance" standard insufficient for the same purpose. This anomaly is avoided by interpreting sections 2702-2703 as implicitly permitting the production of records pursuant to a FISC order issued under section 1861.

It is the Court's responsibility to attempt to interpret a statute "as a symmetrical and coherent regulatory scheme, and fit, if possible, all parts into an harmonious whole." Food & Drug Admin. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 133 (2000) (internal quotations and citations omitted). For the foregoing reasons, the Court is persuaded that this objective is better served by the interpretation that the records sought in this case are obtainable pursuant to a section 1861 order.

However, to the extent that any ambiguity may remain, it should be noted that the legislative history of the USA PATRIOT Act is consistent with this expansive interpretation of section 1861(a)(1). See 147 Cong. Rec. 20,703 (2001) (statement of Sen. Feingold) (section 215 of USA PATRIOT Act "permits the Government . . . to compel the production of records from any business regarding any person if that information is sought in connection with an investigation of terrorism or espionage;" "all business records can be compelled, including those containing sensitive personal information, such as medical records from hospitals or doctors, or educational records, or records of what books somebody has taken out from the library") (emphasis added). In this regard, it is significant that Senator Feingold introduced an amendment to limit the scope of section 1861 orders to records "not protected by any Federal or State law governing access to the records for intelligence or law enforcement purposes," but this limitation was not adopted. See 147 Cong. Rec. 19,530 (2001).

ENTERED this 12th day of December, 2008, regarding Docket No. BR 08-13.


REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

¹⁰(...continued)

person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Id. § 1861(a)(1). The application must also include minimization procedures in conformance with statutory requirements, which must also be reviewed by the FISC. Id. § 1861(b)(2)(B), (c)(1), & (g).

~~TOP SECRET//COMINT//ORCON,NOFORN//MR~~

SIMS DECLARATION
EXHIBIT 5

~~SECRET~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
FOR AN ORDER REQUIRING THE
PRODUCTION OF TANGIBLE THINGS
FROM (b) (1)

Docket No.: BR 10-82

SUPPLEMENTAL ORDER

In granting the application in this matter, the Court has concluded that the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (RFPA), does not preclude the issuance of an order requiring the production of financial records to the Federal Bureau of Investigation (FBI) pursuant to the FISA business records provision, 50 U.S.C. § 1861. This Supplemental Order briefly memorializes the Court's reasons for reaching that conclusion and addresses a separate issue regarding minimization.

The RFPA generally provides that "no Government authority" may obtain "financial records" from a "financial institution" unless one of several exceptions applies. See 12 U.S.C. § 3402; see also *id.* § 3403. Under one of those exceptions, the FBI may, without prior judicial review, compel a financial institution to produce financial records, provided that a designated FBI official has certified that the records are relevant to an authorized foreign intelligence investigation. See 50 U.S.C. § 3414(a)(5)(A). Pursuant to Section 1861, the government may request, and this Court may grant, "an order requiring the production of any tangible things (including books, records, papers, documents, and other items)." 50 U.S.C. § 1861(a)(1) (emphasis added). Section 1861 requires the government to provide the Court with a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to a foreign intelligence investigation, *id.* § 1861(b)(2)(A), and the Court to determine that the application satisfies this requirement, see *id.* § 1861(c)(1), before records are ordered to be produced.

Although the RFPA contains no provision explicitly allowing the production of financial records pursuant to a Section 1861 order, the Court agrees with the government that it would have been anomalous for Congress to have deemed the FBI's application of a "relevance" standard, without prior judicial review, sufficient to obtain records subject to the RFPA, but to have deemed this Court's application of a closely similar "relevance" standard insufficient for the same purpose. The anomaly is avoided by interpreting the RFPA as permitting the production of

~~SECRET~~

~~SECRET~~

records pursuant to a Section 1861 order. See Docket No. BR 08-13, December 12, 2008 Supplemental Opinion (relying on similar reasoning in holding that 18 U.S.C. §§ 2702 and 2703 implicitly permit the production of call detail records pursuant to an order issued under Section 1861).¹



Issued this 23rd day of November, 2010.

A handwritten signature in black ink, appearing to read "John D. Bates", is written above a horizontal line.

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

¹ In granting the application in this matter, the Court did not rely upon 12 U.S.C. § 3413(d), a separate exception to the RFPA that the government also argued-is applicable.
(b) (6), (b) (7)(C)

~~SECRET~~