

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

Docket Number: BR 13-109

On July 18, 2013, a verified Final "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" (Application) was submitted to the Court by the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States

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

Code (U.S.C.), § 1861, as amended (also known as Section 215 of the USA PATRIOT Act),¹ requiring the ongoing daily production to the National Security Agency (NSA) of certain call detail records or “telephony metadata” in bulk.² The Court, after having fully considered the United States Government’s (government) earlier-filed Proposed Application pursuant to Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 9(a),³ and having held an extensive hearing to receive testimony and

¹ “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (“PATRIOT Act”), amended by, “USA PATRIOT Improvement Reauthorization Act of 2005,” Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006); “USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006,” Pub. L. No. 109-178, 120 Stat. 278 (Mar. 9, 2006); and Section 215 expiration extended by “Department of Defense Appropriations Act, 2010,” Pub. L. No. 111-118 (Dec. 19, 2009); “USA PATRIOT—Extension of Sunsets,” Pub. L. No. 111-141 (Feb. 27, 2010); “FISA Sunsets Extension Act of 2011,” Pub. L. No. 112-3 (Feb. 25, 2011); and, “PATRIOT Sunsets Extension Act of 2011,” Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).

² For purposes of this matter, “‘telephony metadata’ includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) 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.” App. at 4. In addition, the Court has explicitly directed that its authorization does not include “the production of cell site location information (CSLI).” Primary Ord. at 3.

³ Prior to scheduling a hearing in this matter, the Court reviewed the Proposed Application and its filed Exhibits pursuant to its standard procedure. Exhibit A consists of a Declaration from the NSA in support of the government’s Application. As Ordered by this Court in Docket No. BR 13-80, Exhibit B is a Renewal Report to describe any significant changes proposed in the way in which records would be received, and any significant changes to controls NSA has in place to receive, store, process, and disseminate the information. [REDACTED] It also provides the final segment of information normally contained in the 30-day reports discussed below. As Ordered by this Court in Docket No. BR 13-80, Exhibit C is a summary of a meeting held by Executive Branch representatives to assess compliance with this Court’s Orders. Furthermore, the Court reviewed the previously filed 30-day reports that were Ordered by this Court in Docket No. 13-80, discussing NSA’s application of the reasonable, articulable suspicion (RAS) standard for approving selection terms and implementation of the automated query process. In addition, the 30-day reports describe disseminations of U.S.-person information obtained under this program.

evidence on this matter on July 18, 2013,⁴ GRANTED the application for the reasons stated in this Memorandum Opinion and in a Primary Order issued on July 19, 2013, which is appended hereto.

In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.

⁴ The proceedings were conducted *ex parte* under security procedures as mandated by 50 U.S.C. §§ 1803(c), 1861(c)(1), and FISC Rules 3, 17(a)-(b). See Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7 (noting that initial proceedings before the FISC are handled *ex parte* as is the universal practice in courts that handle government requests for orders for the production of business records, pen register/trap and trace implementation, wiretaps, and search warrants), <http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf>. Pursuant to FISC Rules 17(b)-(d), this Court heard oral argument by attorneys from the U.S. Department of Justice, and received sworn testimony from personnel from the FBI and NSA. The Court also entered into evidence Exhibits 1-7 during the hearing. Except as cited in this Memorandum Opinion, at the request of the government, the transcript of the hearing has been placed under seal by Order of this Court for security reasons. Draft Tr. at 3-4. At the hearing, the government notified the Court that it was developing an updated legal analysis expounding on its legal position with regard to the application of Section 215 to bulk telephony metadata collection. Draft Tr. at 25. The government was not prepared to present such a document to the Court. The Court is aware that on August 9, 2013, the government released to the public an "Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act" (Aug. 9, 2013). The Court, however, has not reviewed the government's "White Paper" and the "White Paper" has played no part in the Court's consideration of the government's Application or this Memorandum Opinion.

Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). Primary Ord. at 3 n.1.⁵ The government requested production of this data on a daily basis for a period of 90 days. The sole purpose of this production is to obtain foreign intelligence information in support of [REDACTED] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations. See Primary Ord. at 2, 6; App. at 8; and, Ex. A. at 2-3. In granting the government's request, the Court has prohibited the government from accessing the data for any other intelligence or investigative purpose.⁶ Primary Ord. at 4.

⁵ In the event that the government seeks the production of CSLI as part of the bulk production of call detail records in the future, the government would be required to provide notice and briefing to this Court pursuant to FISC Rule 11. The production of all call detail records of all persons in the United States has never occurred under this program. For example, the government [REDACTED] App. at 13 n.4.

⁶ The government may, however, permit access to "trained and authorized technical personnel ... to perform those processes needed to make [the data] usable for intelligence analysis," Primary Ord. at 5, and may share query results "[1] to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate lawful oversight functions." Id. at 14.

By the terms of this Court's Primary Order, access to the data is restricted through technical means, through limits on trained personnel with authorized access, and through a query process that requires a reasonable, articulable suspicion (RAS), as determined by a limited set of personnel, that the selection term (e.g., a telephone number) that will be used to search the data is associated with one of the identified international terrorist organizations.⁷ Primary Ord. at 4-9. Moreover, the government may not make the RAS determination for selection terms reasonably believed to be used by U.S. persons solely based on activities protected by the First Amendment. *Id.* at 9; and see 50 U.S.C. § 1861(a)(1). To ensure adherence to its Orders, this Court has the authority to oversee compliance, see 50 U.S.C. § 1803(h), and requires the government to notify the Court in writing immediately concerning any instance of non-compliance, see FISC Rule 13(b). According to the government, in the prior authorization period there have been no compliance incidents.⁸

Finally, although not required by statute, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international

⁷ A selection term that meets specific legal standards has always been required. This Court has not authorized government personnel to access the data for the purpose of wholesale "data mining" or browsing.

⁸ The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved.

terrorist organizations, see App. Ex. B at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (Jun. 25, 2013) at 3-4; Thirty-Day Report for Filing in Docket Number BR 13-80 (May 24, 2013) a 3-4.

II. Fourth Amendment.⁹

The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in Smith v. Maryland, 442 U.S. 735 (1979). The Smith decision and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years. Specifically, the Smith case involved a Fourth Amendment challenge to the use of a pen register on telephone company equipment to capture information concerning telephone calls,¹⁰ but not the content or the identities of the parties to a conversation. Id. at 737, 741 (citing Katz v. United States, 389 U.S. 347 (1967), and United States v. New York Tel. Co., 434 U.S. 159 (1977)). The same type of information is at issue here.¹¹

⁹ "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

¹⁰ Because the metadata was obtained from telephone company equipment, the Court found that "petitioner obviously cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.'" Id. at 741.

¹¹ The Court is aware that additional call detail data is obtained via this production than was acquired through the pen register acquisition at issue in Smith. Other courts have had the opportunity to review whether there is a Fourth Amendment expectation of privacy in call detail records similar to the data sought in this matter and have found that there is none. See United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (finding that because "data about the 'call origination, length, and time of call' ... is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.'"

The Supreme Court in Smith recognized that telephone companies maintain call detail records in the normal course of business for a variety of purposes. Id. at 742 ("All subscribers realize ... that the phone company has facilities for making permanent records of the number they dial...."). This appreciation is directly applicable to a business records request. "Telephone users ... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." Id. at 743. Furthermore, the Supreme Court found that once a person has transmitted this information to a third party (in this case, a telephone company), the person "has no legitimate expectation of privacy in [the] information...."¹² Id. The telephone user, having conveyed this information to a telephone company that retains the information in the ordinary course of business, assumes the risk that the company will provide that information to the

(citing Smith, 442 U.S. at 743-44)) cert. denied 559 U.S. 987, 988 (2010); United States Telecom Ass'n, 227 F.3d 450, 454 (D.C. Cir. 2000) (noting pen registers record telephone numbers of outgoing calls and trap and trace devices are like caller ID systems, and that such information is not protected by the Fourth Amendment); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990) (recognizing that "[t]he installation and use of a pen register and trap and trace device is not a 'search' requiring a warrant pursuant to the Fourth Amendment," and noting that there is no "'legitimate expectation of privacy' at stake." (citing Smith, 442 U.S. at 739-46)).

¹² The Supreme Court has applied this principle – that there is no Fourth Amendment search when the government obtains information that has been conveyed to third parties – in cases involving other types of business records. See United States v. Miller, 425 U.S. 435 (1976) (bank records); see also S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities.") (citing Miller, 425 U.S. at 443).

government. See id. at 744. Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it "was not a 'search,' and no warrant was required" under the Fourth Amendment. Id. at 746.¹³

In Smith, the government was obtaining the telephone company's metadata of one person suspected of a crime. See id. at 737. Here, the government is requesting daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [REDACTED]

[REDACTED] In that case, this Court found that "regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy." Id. at 62. The Court noted that Fourth Amendment rights are personal and individual, see id. (citing Steagald v. United States, 451 U.S. 204, 219 (1981); accord, e.g., Rakas v. Illinois, 439 U.S. 128, 133 (1978) ("Fourth Amendment rights are personal rights which ... may not be vicariously asserted.")) (quoting Alderman v. United States, 394 U.S. 165, 174 (1969))), and that "[s]o long as no individual has a reasonable expectation of privacy

¹³ If a service provider believed that a business records order infringed on its own Fourth Amendment rights, it could raise such a challenge pursuant to 50 U.S.C. § 1861(f).

in meta data, the large number of persons whose communications will be subjected to the ... surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." *Id.* at 63. Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.

In sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, Smith v. Maryland compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in [REDACTED] and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise.

III. Section 215.

Section 215 of the USA PATRIOT Act created a statutory framework, the various parts of which are designed to ensure not only that the government has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information. It requires the government to demonstrate, among other things, that there is "an investigation to

obtain foreign intelligence information ... to [in this case] protect against international terrorism," 50 U.S.C. § 1861(a)(1); that investigations of U.S. persons are "not conducted solely upon the basis of activities protected by the first amendment to the Constitution," id.; that the investigation is "conducted under guidelines approved by the Attorney General under Executive Order 12333," id. § 1861(a)(2); that there is "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to the investigation, id. § 1861(b)(2)(A);¹⁴ that there are adequate minimization procedures "applicable to the retention and dissemination" of the information requested, id. § 1861(b)(2)(B); and, that only the production of such things that could be "obtained with a subpoena *duces tecum*" or "any other order issued by a court of the United States directing the production of records" may be ordered, id. § 1861(c)(2)(D), see infra Part III.a. (discussing Section 2703(d) of the Stored Communications Act). If the Court determines that the government has met the requirements of Section 215, it shall enter an *ex parte* order compelling production.¹⁵

¹⁴ This section also provides that the records sought are "presumptively relevant to an authorized investigation if the applicant shows in the statement of facts that they pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known, to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. § 1861(b)(2)(A)(i)-(iii). The government has not invoked this presumption and, therefore, the Court need not address it.

¹⁵ "Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of [Section 215], the judge *shall* enter an *ex parte* order as requested, or as modified, approving the release of tangible things." Id. § 1861(c)(1) (emphasis added). As indicated, the Court may modify the Orders as necessary, and compliance issues could present situations requiring modification.

This Court must verify that each statutory provision is satisfied before issuing the requested Orders. For example, even if the Court finds that the records requested are relevant to an investigation, it may not authorize the production if the minimization procedures are insufficient. Under Section 215, minimization procedures are "specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." Id. § 1861(g)(2)(A). Congress recognized in this provision that information concerning U.S. persons that is not directly responsive to foreign intelligence needs will be produced under these orders and established post-production protections for such information. As the Primary Order issued in this matter demonstrates, this Court's authorization includes detailed restrictions on the government through minimization procedures. See Primary Ord. at 4-17. Without those restrictions, this Court could not, nor would it, have approved the proposed production. This Court's Primary Order also sets forth the requisite findings under Section 215 for issuing the Orders requested by the government in its Application. Id. at 2, 4-17.

The Court now turns to its interpretation of Section 215 with regard to how it compares to 18 U.S.C. § 2703 (Stored Communications Act); its determination that “there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation,” 50 U.S.C. § 1861(b)(2)(A); and, the doctrine of legislative re-enactment as it pertains to the business records provision.

- a. Section 215 of FISA and Section 2703(d) of the Stored Communications Act.

It is instructive to compare Section 215, which is used for foreign intelligence purposes and is codified as part of FISA, with 18 U.S.C. § 2703 (“Required disclosure of customer communications or records”), which is used in criminal investigations and is part of the Stored Communications Act (SCA). See In Re Production of Tangible Things From [REDACTED]

[REDACTED], Docket No. BR 08-13, Supp. Op. (Dec. 12, 2008) (discussing Section 215 and Section 2703). Section 2703 establishes a process by which the government can obtain information from electronic communications service providers, such as telephone companies. As with FISA, this section of the SCA provides the mechanism for obtaining either the contents of communications, or non-content records of communications. See 18 U.S.C. §§ 2703(a)-(c).

For non-content records production requests, such as the type sought here, Section 2703(c) provides a variety of mechanisms, including acquisition through a court order under Section 2703(d). Under this section, which is comparable to Section 215, the government must offer to the court “*specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation.*” *Id.* § 2703(d) (emphasis added). Section 215, the comparable provision for foreign intelligence purposes, requires neither “specific and articulable facts” nor does it require that the information be “material.” Rather, it merely requires a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to the investigation. See 50 U.S.C. §1861(b)(2)(A). That these two provisions apply to the production of the same type of records from the same type of providers is an indication that Congress intended this Court to apply a different, and in specific respects lower, standard to the government’s Application under Section 215 than a court reviewing a request under Section 2703(d). Indeed, the pre-PATRIOT Act version of FISA’s business records provision required “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.” 50 U.S.C. §1862(b)(2)(B) as it read on October 25, 2001.¹⁶ In enacting Section 215,

¹⁶ Prior to enactment of the PATRIOT Act, the business records provision was in Section 1862 vice 1861.

Congress removed the requirements for "specific and articulable facts" and that the records pertain to "a foreign power or an agent of a foreign power." Accordingly, now the government need not provide specific and articulable facts, demonstrate any connection to a particular suspect, nor show materiality when requesting business records under Section 215. To find otherwise would be to impose a higher burden – one that Congress knew how to include in Section 215, but chose to dispense with.

Furthermore, Congress provided different measures to ensure that the government obtains and uses information properly, depending on the purpose for which it sought the information. First, Section 2703 has no provision for minimization procedures. However, such procedures are mandated under Section 215 and must be designed to restrict the retention and dissemination of information, as imposed by this Court's Primary Order. Primary Ord. at 4-17; see 50 U.S.C. §§ 1861(c)(1), (g).

Second, Section 2703(d) permits the service provider to file a motion with a court to "quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause undue burden on such provider." Id. Congress recognized that, even with the higher statutory standard for a production order under Section 2703(d), some requests authorized by a court would be "voluminous" and provided a means by which the provider could seek relief using a motion. Id. Under Section 215, however, Congress

provided a specific and complex statutory scheme for judicial review of an Order from this Court to ensure that providers could challenge both the legality of the required production and the nondisclosure provisions of that Order. 50 U.S.C. § 1861(f). This adversarial process includes the selection of a judge from a pool of FISC judges to review the challenge to determine if it is frivolous and to rule on the merits, *id.* § 1861(f)(2)(A)(ii), provides standards that the judge is to apply during such review, *id.* §§ 1861(f)(2)(B)-(C), and provides for appeal to the Foreign Intelligence Surveillance Court of Review and, ultimately, the U.S. Supreme Court, *id.* § 1861(f)(3).¹⁷ This procedure, as opposed to the motion process available under Section 2703(d) to challenge a production as unduly voluminous or burdensome, contemplates a substantial and engaging adversarial process to test the legality of this Court's Orders under Section 215.¹⁸ This enhanced process appears designed to ensure that there are additional safeguards in light of the lower threshold that the government is required to meet for production under Section 215 as opposed to Section 2703(d). To date, no holder of

¹⁷ For further discussion on the various means by which adversarial proceedings before the FISC may occur, *see* Letter from Presiding Judge Walton, U.S. FISC to Chairman Leahy, Senate Judiciary Committee (Jul. 29, 2013), at 7-10, <http://www.uscourts.gov/uscourts/fisc/honorable-patrick-leahy.pdf>.

¹⁸ In *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F.Supp.2d 114, 128-29 (E.D. Va. 2011), the court found that only the service provider, as opposed to a customer or subscriber, could challenge the execution of a § 2703(d) non-content records order. The court reasoned that "[b]ecause Congress clearly provided ... protections for one type of § 2703 order [content] but not for others, the Court must infer that Congress deliberately declined to permit challenges for the omitted orders." *Id.* The court also noted that the distinction between content and non-content demonstrates an incorporation of *Smith v. Maryland* into the SCA. *Id.* at 128 n.11. As discussed above, the operation of Section 215 within FISA represents that same distinction.

records who has received an Order to produce bulk telephony metadata has challenged the legality of such an Order. Indeed, no recipient of any Section 215 Order has challenged the legality of such an Order, despite the explicit statutory mechanism for doing so.

When analyzing a statute or a provision thereof, a court considers the statutory schemes as a whole. See Kokoszka v. Belford, 417 U.S. 642, 650 (1974) (noting that when a court interprets a statute, it looks not merely to a particular clause but will examine it within the whole statute or statutes on the same subject) (internal quotation and citation omitted); Jones v. St. Louis-San Francisco Ry. Co., 728 F.2d 257, 262 (6th Cir. 1984) (“[W]here two or more statutes deal with the same subject, they are to be read *in pari materia* and harmonized, if possible. This rule of statutory construction is based upon the premise that when Congress enacts a new statute, it is aware of all previously enacted statutes on the same subject.”) (citations omitted). Here, the Court finds that Section 215 and Section 2703(d) operate in a complementary manner and are designed for their specific purposes. In the criminal investigation context, Section 2703(d) includes front-end protections by imposing a higher burden on the government to obtain the information in the first instance. On the other hand, when the government seeks to obtain the same type of information, but for a foreign intelligence purpose, Congress provided the government with more latitude at the production stage under

Section 215 by not requiring specific and articulable facts or meeting a materiality standard. Instead, it imposed post-production checks in the form of mandated minimization procedures and a structured adversarial process. This is a logical framework and it comports well with the Fourth Amendment concept that the required factual predicate for obtaining information in a case of special needs, such as national security, can be lower than for use of the same investigative measures for an ordinary criminal investigation. See United States v. United States District Court (Keith), 407 U.S. 297, 308-09, 322-23 (1972); and, In re Sealed Case, 310 F.3d 717, 745-46 (FISA Ct. Rev. 2002) (differentiating requirements for the government to obtain information obtained for national security reasons as opposed to a criminal investigation).¹⁹ Moreover, the government's interest is significantly greater when it is attempting to thwart attacks and disrupt activities that could harm national security, as opposed to gathering evidence on domestic crimes. See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("[T]he relevant government interest—the interest in national security—is of the highest order of magnitude.") (citing Haig v. Agee, 453 U.S. 280, 307 (1981)); and, In re Sealed Case, 310 F.3d at 745-46.

¹⁹ As discussed above, there is no Fourth Amendment interest here, as per Smith v. Maryland.

b. Relevance.

Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.

As an initial matter and as a point of clarification, the government's burden under Section 215 is not to prove that the records sought are, in fact, relevant to an authorized investigation. The explicit terms of the statute require "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant...." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). In establishing this standard, Congress chose to leave the term "relevant" undefined. It is axiomatic that when Congress declines to define a term a court must give the term its ordinary meaning. See, e.g., Taniguchi v. Kan Pacific Saipan, Ltd., ___ U.S. ___, 132 S.Ct. 1997, 2002 (2012). Accompanying the government's first application for the bulk production of telephone company metadata was a Memorandum of Law which argued that "[i]nformation is 'relevant' to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation." Mem. of Law in Support of App. for Certain Tangible

Things for Investigations to Protect Against International Terrorism, Docket No. BR 06-05 (filed May 23, 2006), at 13-14 (quoting dictionary definitions, Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978), and Fed. R. Evid. 401²⁰). This Court recognizes that the concept of relevance here is in fact broad and amounts to a relatively low standard.²¹ Where there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations.

This Court has previously examined the issue of relevance for bulk collections.

See [REDACTED]
[REDACTED]
[REDACTED]

²⁰ At the time of the government's submission in Docket No. BR 06-05, a different version of Fed. R. Evid. 401 was in place. While not directly applicable in this context, the current version reads: "Evidence is relevant if: (a) it has *any tendency* to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." (Emphasis added.)

²¹ Even under the higher "relevant and material" standard for 18 U.S.C. § 2703(d), discussed above, "[t]he government need not show actual relevance, such as would be required at trial." In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F.Supp.2d 114, 130 (E.D. Va. 2011). The petitioners had argued in that case that most of their activity for which records were sought was "unrelated" and that "the government cannot be permitted to blindly request everything that 'might' be useful..." Id. (internal quotation omitted). The court rejected this argument, noting that "[t]he probability that some gathered information will not be material is not a substantial objection," and that where no constitutional right is implicated, as is the case here, "there is no need for ... narrow tailoring." Id.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] While those matters involved different collections from the one at issue here, the relevance standard was similar. See 50 U.S.C. § 1842(c)(2) ("[R]elevant to an ongoing investigation to protect against international terrorism...."). In both cases, there were facts demonstrating that information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain. As this Court noted in 2010, the "finding of relevance most crucially depended on the conclusion that bulk collection is *necessary* for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives." [REDACTED]

[REDACTED]

[REDACTED] Indeed, in [REDACTED] this Court noted that bulk collections such as these are "necessary to identify the much smaller number of [international terrorist] communications." [REDACTED]

As a result, it is this showing of necessity that led the Court to find that "the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons." [REDACTED]

This case is no different. The government stated, and this Court is well aware, that individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including within the United States. Ex. A. at 4. The government argues that the broad collection of telephone company metadata “is necessary to create a historical repository of metadata that enables NSA to find or identify known *and unknown* operatives ..., some of whom may be in the United States or in communication with U.S. persons.” App. at 6 (emphasis added). The government would use such information, in part, “to detect and prevent terrorist acts against the United States and U.S. interests.” Ex. A. at 3. The government posits that bulk telephonic metadata is necessary to its investigations because it is impossible to know where in the data the connections to international terrorist organizations will be found. *Id.* at 8-9. The government notes also that “[a]nalysts know that the terrorists’ communications are located somewhere” in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries. *Id.* As the government stated in its 2006 Memorandum of Law, “[a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection.” Mem. of Law at 15, Docket No. BR 06-05.

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

The government depends on this bulk collection because if production of the information were to wait until the specific identifier connected to an international terrorist group were determined, most of the historical connections (the entire purpose of this authorization) would be lost. See Ex. A. at 7-12. The analysis of past connections is only possible "if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related." Mem. of Law at 2, Docket No. BR 06-05. Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.

The government must demonstrate "facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. 1861(b)(2)(A). The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to

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

obtain a production of records. Furthermore, it is important to remember that the relevance finding is only one part of a whole protective statutory scheme. Within the whole of this particular statutory scheme, the low relevance standard is counter-balanced by significant post-production minimization procedures that must accompany such an authorization and an available mechanism for an adversarial challenge in this Court by the record holder. See supra Part III.a. Without the minimization procedures set out in detail in this Court's Primary Order, for example, no Orders for production would issue from this Court. See Primary Ord. at 4-17. Taken together, the Section 215 provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged. The Application before this Court fits comfortably within this statutory framework.

c. Legislative Re-enactment or Ratification.

As the U.S. Supreme Court has stated, "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." Lorillard v. Pons, 434 U.S. 575, 580 (1978) (citing cases and authorities); see also Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239-40 (2009) (quoting Lorillard, 434 U.S. at 580). This doctrine of legislative re-enactment,

also known as the doctrine of ratification, is applicable here because Congress re-authorized Section 215 of the PATRIOT Act without change in 2011. "PATRIOT Sunsets Extension Act of 2011," Pub. L. No. 112-14, 125 Stat. 216 (May 26, 2011).²² This doctrine applies as a presumption that guides a court in interpreting a re-enacted statute. See Lorillard, 434 U.S. at 580-81 (citing cases); NLRB v. Gullett Gin Co., 340 U.S. 361, 365-66 (1951) ("[I]t is a fair assumption that by reenacting without pertinent modification ... Congress accepted the construction ... approved by the courts."); 2B Sutherland on Statutory Construction § 49:8 and cases cited (7th ed. 2009). Admittedly, in the national security context where legal decisions are classified by the Executive Branch and, therefore, normally not widely available to Members of Congress for scrutiny, one could imagine that such a presumption would be easily overcome. However, despite the highly-classified nature of the program and this Court's orders, that is not the case here.

Prior to the May 2011 congressional votes on Section 215 re-authorization, the Executive Branch provided the Intelligence Committees of both houses of Congress with letters which contained a "Report on the National Security Agency's Bulk

²² The Senate and House of Representatives voted to re-authorize Section 215 for another four years by overwhelming majorities. See http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=1&vote=00084 (indicating a 72-23 vote in the Senate); and, <http://clerk.house.gov/evs/2011/roll376.xml> (indicating a 250-153 vote in the House). President Obama signed the re-authorization into law on May 26, 2011.

Collection Programs for USA PATRIOT Act Reauthorization" (Report). Ex. 3 (Letter to Hon. Mike Rogers, Chairman, and Hon. C.A. Dutch Ruppersberger, Ranking Minority Member, Permanent Select Committee on Intelligence, U.S. House of Representatives (HPSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (HPSCI Letter); and, Letter to Hon. Dianne Feinstein, Chairman, and Hon. Saxby Chambliss, Vice Chairman, Select Committee on Intelligence, U.S. Senate (SSCI), from Ronald Weich, Asst. Attorney General (Feb. 2, 2011) (SSCI Letter)). The Report provided extensive and detailed information to the Committees regarding the nature and scope of this Court's approval of the implementation of Section 215 concerning bulk telephone metadata.²³ The Report noted that "[a]lthough these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about th[is] ... program[] when considering reauthorization of the

²³ Specifically, the Report provided the following information: 1) the Section 215 production is a program "authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls ... but not the content of the calls" Ex. 3, Report at 1 (emphasis in original); 2) this Court's "orders generally require production of the business records (as described above) relating to *substantially all of the telephone calls* handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States," *id.* at 3 (emphasis added); 3) "Although the program[] collect[s] a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes," *id.* at 1; 4) "The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress," *id.*; 5) "Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court," *id.*; 6) "Today, under FISA Court authorization pursuant to the 'business records' authority of the FISA (commonly referred to as 'Section 215'), the government has developed a program to close the gap" regarding a terrorist plot, *id.* at 2; 7) "NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States," *id.*; and, 8) that the program operates "on a very large scale." *Id.*

expiring PATRIOT Act provisions.” *Id.* Report at 3. Furthermore, the government stated the following in the HPSCI and SSCI Letters: “We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215....” *Id.* HPSCI Letter at 1; SSCI Letter at 1. It is clear from the letters that the Report would be made available to *all* Members of Congress and that HPSCI, SSCI, and Executive Branch staff would also be made available to answer any questions from Members of Congress.²⁴ *Id.* HPSCI Letter at 2; SSCI Letter at 2.

In light of the importance of the national security programs that were set to expire, the Executive Branch and relevant congressional committees worked together to ensure that *each* Member of Congress knew or had the opportunity to know how

²⁴ It is unnecessary for the Court to inquire how many of the 535 individual Members of Congress took advantage of the opportunity to learn the facts about how the Executive Branch was implementing Section 215 under this Court’s Orders. Rather, the Court looks to congressional action on the whole, not the preparatory work of individual Members in anticipation of legislation. In fact, the Court is bound to presume regularity on the part of Congress. *See City of Richmond v. J.A. Croson Co.*, 488 U.S. 469, 500 (1989) (“The factfinding process of legislative bodies is generally entitled to a presumption of regularity and deferential review by the judiciary.” (citing cases)). The ratification presumption applies here where each Member was presented with an opportunity to learn about a highly-sensitive classified program important to national security in preparation for upcoming legislative action. Furthermore, Congress as a whole may debate such legislation in secret session. *See* U.S. Const. art. I, Sec. 5. (“Each House may determine the Rules of its Proceedings, Each House shall keep a Journal of its Proceedings, and from time to time publish the same *excepting such Parts as may in their Judgment require Secrecy*;”) (emphasis added.). In fact, according to a Congressional Research Service Report, both Houses have implemented rules for such sessions pursuant to the Constitution. *See* “Secret Sessions of the House and Senate: Authority, Confidentiality, and Frequency” Congressional Research Service (Mar. 15, 2013), at 1-2 (citing House Rules XVII, cl. 9; X, cl. 11; and, Senate Rules XXI; XXIX; and, XXXI). Indeed, both Houses have entered into secret session in the past decade to discuss intelligence matters. *See id.* at 5 (Table 1. Senate “Iraq war intelligence” (Nov. 1, 2005); Table 2. House of Representatives “Foreign Intelligence Surveillance Act and electronic surveillance” (Mar. 13, 2008)).

Section 215 was being implemented under this Court's Orders.²⁵ Documentation and personnel were also made available to afford each Member full knowledge of the scope of the implementation of Section 215 and of the underlying legal interpretation.

The record before this Court thus demonstrates that the factual basis for applying the re-enactment doctrine and presuming that in 2011 Congress intended to ratify Section 215 as applied by this Court is well supported. Members were informed that this Court's "orders generally require production of the business records (as described above) relating to *substantially all of the telephone calls* handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States." Ex. 3, Report at 3 (emphasis added). When Congress subsequently re-authorized Section 215 without change, except as to expiration date, that re-authorization carried with it this Court's interpretation of the statute, which permits the bulk collection of telephony metadata under the restrictions that are in place. Therefore, the passage of the PATRIOT Sunsets Extension Act

²⁵ Indeed, one year earlier when Section 215 was previously set to expire, SSCI Chairman Feinstein and Vice Chairman Bond sent a letter to every Senator inviting "each Member of the Senate" to read a very similar Report to the one provided in the 2011 Letters, and pointing out that this would "permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote." Ex. 7 ("Dear Colleague" Letter from SSCI Chairman Dianne Feinstein and Vice Chairman Christopher Bond (Feb. 23, 2010)). The next day, HPSCI Chairman Reyes sent a similar notice to each Member of the House that this information would be made available "on important intelligence collection programs made possible by these expiring authorities." Ex. 2 ("Dear Colleague" Notice from HPSCI Chairman Silvestre Reyes (Feb. 24, 2010)). This notice also indicated that the HPSCI Chairman and Chairman Conyers of the House Judiciary Committee would "make staff available to meet with any member who has questions" along with Executive Branch personnel. *Id.*

provides a persuasive reason for this Court to adhere to its prior interpretations of Section 215.

IV. Conclusion.

This Court is mindful that this matter comes before it at a time when unprecedented disclosures have been made about this and other highly-sensitive programs designed to obtain foreign intelligence information and carry out counter-terrorism investigations. According to NSA Director Gen. Keith Alexander, the disclosures have caused "significant and irreversible damage to our nation." Remarks at "Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War," Aspen, Colo. (Jul. 18, 2013). In the wake of these disclosures, whether and to what extent the government seeks to continue the program discussed in this Memorandum Opinion is a matter for the political branches of government to decide.

As discussed above, because there is no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention to the statute. The Court concludes that there are facts showing reasonable grounds to believe that the records sought are relevant to authorized investigations. This conclusion is supported not only by the plain text and structure of Section 215, but also by the statutory modifications

and framework instituted by Congress. Furthermore, the Court finds that this result is strongly supported, if not required, by the doctrine of legislative re-enactment or ratification.

For these reasons, for the reasons stated in the Primary Order appended hereto, and pursuant to 50 U.S.C. § 1861(c)(1), the Court has GRANTED the Orders requested by the government.

Because of the public interest in this matter, pursuant to FISC Rule 62(a), the undersigned FISC Judge requests that this Memorandum Opinion and the Primary Order of July 19, 2013, appended herein, be published, and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 29th day of August, 2013.



CLAIRE V. EAGAN

Judge, United States Foreign
Intelligence Surveillance Court

~~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]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Docket Number: BR 13-109

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: [REDACTED]

~~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 BR 13-80 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

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

Accordingly, and as further explained in a Memorandum Opinion to follow, 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. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

~~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

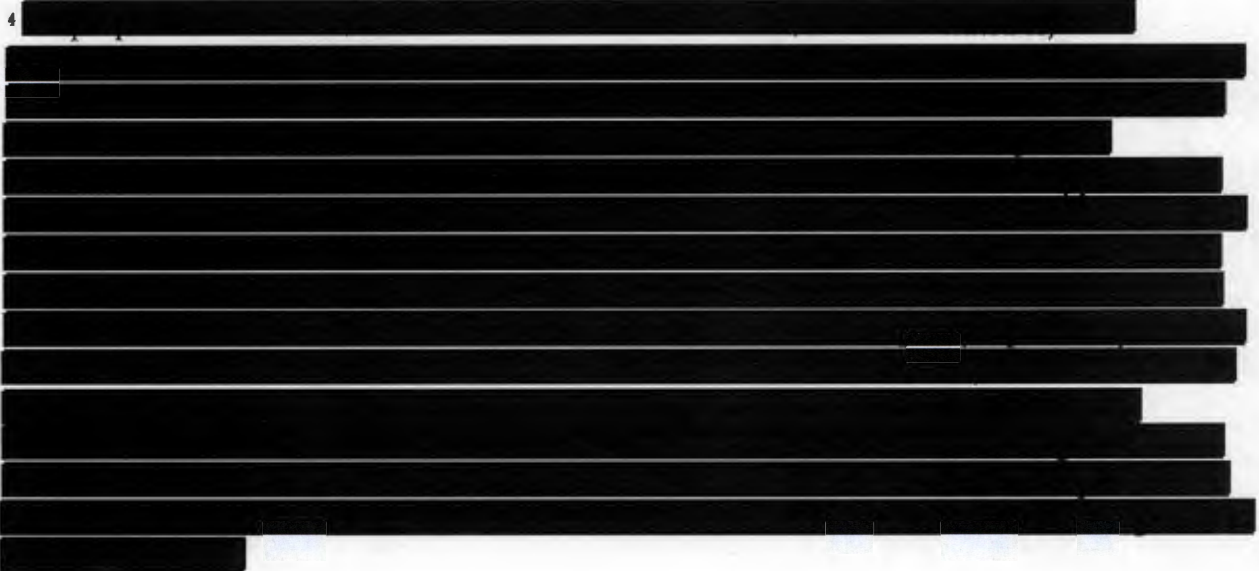
that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate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

⁴



~~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 queries of the BR metadata to obtain contact chaining information 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

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~~

adequate and 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]

[REDACTED]

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

[REDACTED]

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

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

[REDACTED]

~~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] solely 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]

[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~~

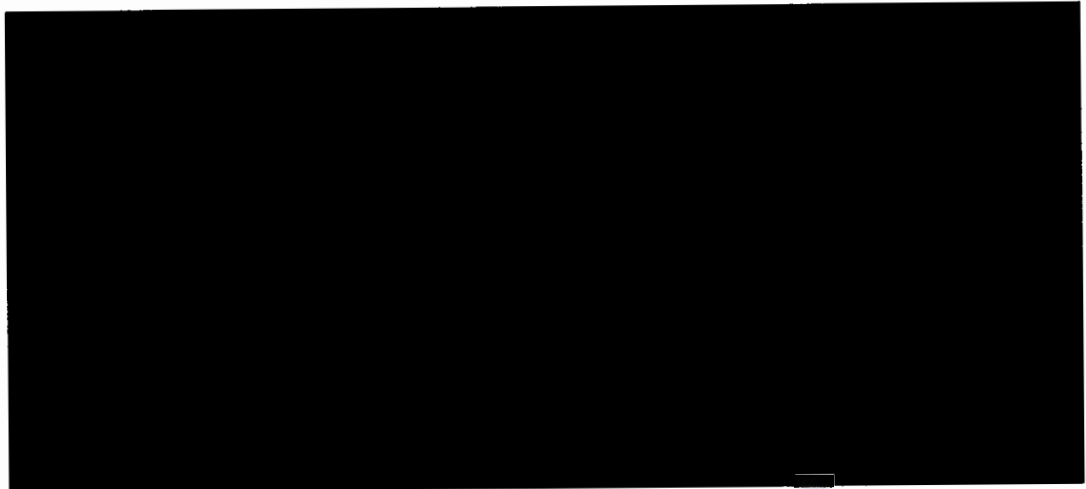
pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated [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.

¹⁰ The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Order. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

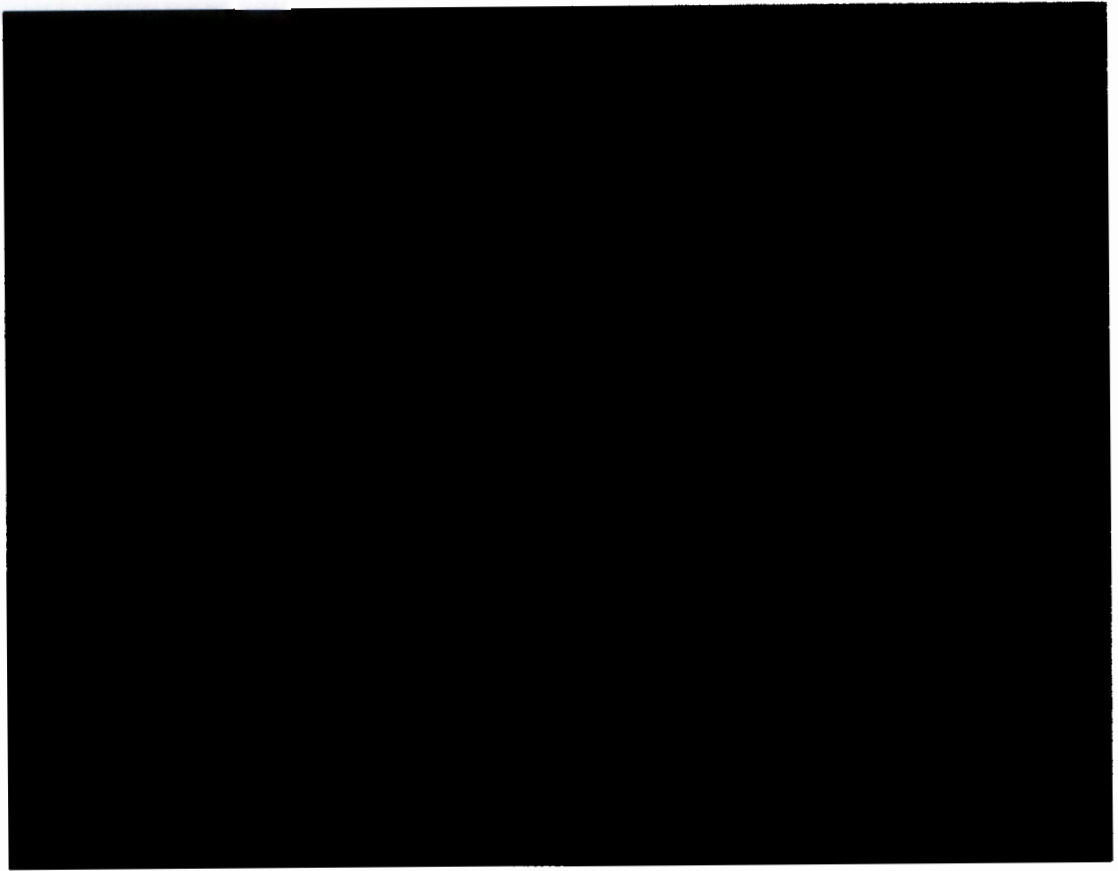
(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.¹¹ This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns 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:



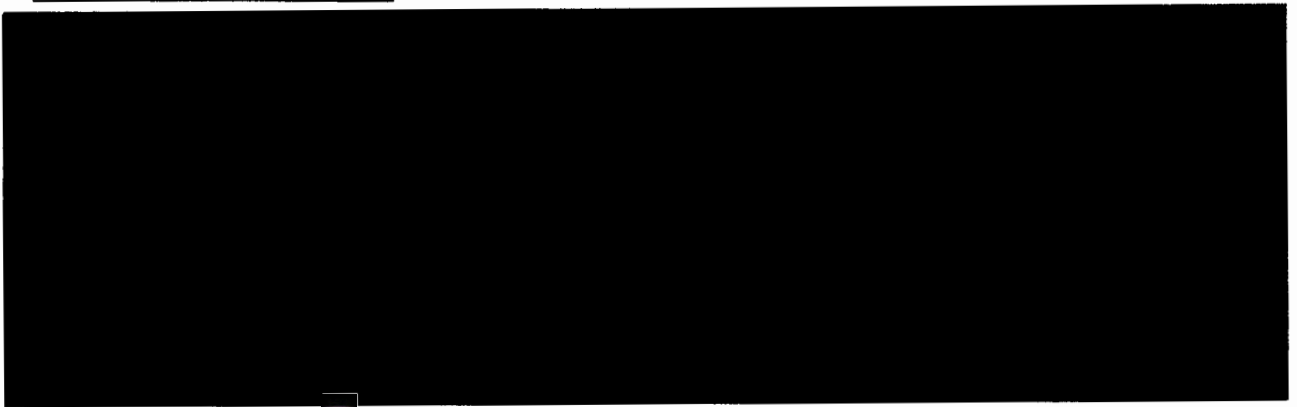
¹¹ This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

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~~



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



~~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.

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~~

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~~

(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) Other than the automated query process described in the [REDACTED] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified 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 and operation 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

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

authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

This authorization regarding

[REDACTED]

expires on the 11th day

of October, 2013, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time

Y12-9-1017 110:43

Claire V. Eagan

CLAIRE V. EAGAN

Judge, United States Foreign
Intelligence Surveillance Court

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