

No. 14-35555

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ANNA J. SMITH

Plaintiff-Appellant,

v.

BARACK OBAMA et al.,

Defendant-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT
COURT FOR THE DISTRICT OF IDAHO

BRIEF FOR THE APPELLEES

JOYCE R. BRANDA
*Acting Assistant Attorney
General*

WENDY J. OLSON
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
HENRY C. WHITAKER
*(202) 514-3180
Attorneys, Appellate Staff
Civil Division, Room 7256
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530*

TABLE OF CONTENTS

INTRODUCTION.....	1
STATEMENT OF JURISDICTION.....	3
STATEMENT OF THE ISSUES.....	3
PERTINENT STATUTES AND REGULATIONS	4
STATEMENT OF THE CASE	4
I. Nature Of The Case	4
II. Statutory Background.....	5
A. Section 215	5
B. The Section 215 Bulk Telephony- Metadata Program	8
III. Proceedings Below.....	19
A. This Suit.....	19
B. The District Court’s Opinion	21
SUMMARY OF ARGUMENT.....	22
STANDARD OF REVIEW.....	28
ARGUMENT	29
I. Plaintiff Lacks Standing To Challenge The Section 215 Bulk Telephony- Metadata Program	29

II.	The Fourth Amendment Permits The Government To Maintain The Section 215 Program	37
A.	Plaintiff Has No Fourth Amendment Privacy Interest In Business Records Of Verizon Wireless That Contain Telephony Metadata	37
B.	If Obtaining Metadata Implicated A Fourth Amendment Privacy Interest, The Program Would Still Be Constitutional	60
III.	There Is No Basis For Entering A Preliminary Injunction	68
	CONCLUSION	71

TABLE OF AUTHORITIES

Cases	Page
<i>ACLU v. Clapper</i> , 959 F. Supp. 2d 724 (S.D.N.Y. 2013)	38, 42
<i>Alliance for the Wild Rockies v. Cottrell</i> , 632 F.3d 1127 (9th Cir. 2011)	29
<i>Atwater v. City of Lago Vista</i> , 532 U.S. 318 (2001)	40, 45
<i>Bd. of Educ. v. Earls</i> , 536 U.S. 822 (2002)	65, 68
<i>California v. Greenwood</i> , 486 U.S. 35 (1988)	44
<i>Cassidy v. Chertoff</i> , 471 F.3d 67 (2d Cir. 2006).....	61, 66
<i>City of Ontario v. Quon</i> , 560 U.S. 746 (2010)	67
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013)	29, 30, 31, 35
<i>Coons v. Lew</i> , 2014 WL 3866475 (9th Cir. Aug. 7, 2014)	31
<i>DaimlerChrysler Corp. v. Cuno</i> , 547 U.S. 332 (2006)	31
<i>Delaware v. Prouse</i> , 440 U.S. 648 (1979)	48

Donovan v. Lone Steer, Inc.,
464 U.S. 408 (1984) 40

Dorfmann v. Boozer,
414 F.2d 1168 (D.C. Cir. 1969)..... 70

Electronic Frontier Found. v. Dep’t of Justice,
2014 WL 3945646 (N.D. Cal. Aug. 11, 2014) 33

Golden Gate Restaurant Ass’n v. San Francisco,
546 F.3d 639 (9th Cir. 2008) 42

Haig v. Agee,
453 U.S. 280 (1981) 64

Holder v. Humanitarian Law Project,
130 S. Ct. 2705 (2010) 68

In re Application of U.S. for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013) 58

In re Directives,
551 F.3d 1004 (FISC-R 2008)..... 64

In re Grand Jury Proceedings,
827 F.2d 301 (8th Cir. 1987) 47

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*,
No. 14-5004 (D.C. Cir. Jan. 3, 2014) 5, 21, 37, 42, 66

Laird v. Tatum,
408 U.S. 1 (1972) 35, 56

Lopez v. United States,
373 U.S. 427 (1963) 46, 56

MacWade v. Kelly,
460 F.3d 260 (2d Cir. 2006)..... 61, 66

Maryland v. King,
133 S. Ct. 1958 (2013) 64, 65

Mayfield v. United States,
599 F.3d 964 (9th Cir. 2010) 32

Mich. Dep’t of State Police v. Sitz,
496 U.S. 444 (1990) 48, 61, 65, 68

Minnesota v. Carter,
525 U.S. 83 (1998) 46, 55

Nat’l Treasury Emps. Union v. Von Raab,
489 U.S. 656 (1989) 61, 66

Okla. Press Publ’g Co. v. Walling,
327 U.S. 186 (1946) 41

Rakas v. Illinois,
439 U.S. 128 (1978) 46

Riley v. California,
134 S. Ct. 2473 (2014) 26, 51, 52

Smith v. Maryland,
442 U.S. 735 (1979) *passim*

Steagald v. United States,
451 U.S. 204 (1981) 46

Susan B. Anthony List v. Driehaus,
134 S. Ct. 2334 (2014) 31

United States v. Cormier,
220 F.3d 1103 (9th Cir. 2000) 43, 58

United States v. Davis,
 754 F.3d 1205 (11th Cir. 2014), *vacated by*
 2014 WL 4358411 (11th Cir. Sept. 4, 2014)..... 59

United States v. Dionisio,
 410 U.S. 1 (1973) 41, 47

United States v. Forrester,
 512 F.3d 500 (9th Cir. 2008) 50, 58

United States v. Golden Valley Electric Ass’n,
 689 F.3d 1108 (9th Cir. 2012) 41, 43, 63

United States v. Jacobsen,
 466 U.S. 109 (1984) 36, 55

United States v. Jones,
 132 S. Ct. 945 (2012) 48, 49, 59

United States v. Maynard,
 615 F.3d 544 (D.C. Cir. 2010), *aff’d on other grounds*
sub nom. United States v. Jones, 132 S. Ct. 945 (2012) 48, 49

United States v. Miller,
 425 U.S. 435 (1976) 43, 56, 57

United States v. Moalin,
 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013)..... 38

United States v. Place,
 462 U.S. 696 (1983) 36, 55

United States v. Reed,
 575 F.3d 900 (9th Cir. 2009) 50

United States v. U.S. Dist. Court,
 407 U.S. 297 (1972) 61

United States v. Young,
 573 F.3d 711 (9th Cir. 2009) 58

Vernonia Sch. Dist. 47J v. Acton,
 515 U.S. 646 (1995) 60, 65, 68

Whitmore v. Arkansas,
 495 U.S. 149 (1990) 31

Winter v. Natural Res. Def. Council,
 555 U.S. 7 (2008) 28, 29, 36, 69

Constitution

U.S. Const. amend. IV 64

Statutes

28 U.S.C. § 1291 3

28 U.S.C. § 1331 3

50 U.S.C. § 1801(i)..... 15

50 U.S.C. § 1803(a)..... 6

50 U.S.C. § 1808 8

50 U.S.C. § 1826 8

50 U.S.C. § 1846 8

50 U.S.C. § 1861 1, 3, 6, 62

50 U.S.C. § 1861(a)..... 41

50 U.S.C. § 1861(a)(1)..... 6

50 U.S.C. § 1861(a)(2)(A)..... 7

50 U.S.C. § 1861(b)(2)..... 60

50 U.S.C. § 1861(b)(2)(A)..... 6, 7

50 U.S.C. § 1861(b)(2)(B)..... 7

50 U.S.C. § 1861(c)(1)..... 7, 12, 60

50 U.S.C. § 1861(f)(2) 7

50 U.S.C. § 1861(f)(3) 7

50 U.S.C. § 1861(g)..... 12, 60

50 U.S.C. § 1861 note 19, 62

50 U.S.C. § 1862(a)..... 8

50 U.S.C. § 1862(b)..... 8

50 U.S.C. § 1862(c) 8

50 U.S.C. § 1871(a)(4)..... 8

Orders

*In re Application of the FBI for an Order
Requiring the Production of Tangible Things*, Dkt. No. BR-14-01
(FISC Jan. 3, 2014) 11

*In re Application of the FBI for an Order Requiring the
Production of Tangible Things*, Dkt. No. BR-14-01
(FISC Feb. 5, 2014) 17

In re Application of the FBI for an Order Requiring the Production of Tangible Things, Dkt. No. BR-14-01 (FISC Mar. 20, 2014)..... 38, 45, 47

In re Application of the FBI for an Order Requiring the Production of Tangible Things, Dkt. No. BR-14-67 (FISC Mar. 28, 2014)..... 11

In re Application of the FBI for an Order Requiring the Production of Tangible Things, Dkt. No. BR-14-96 (FISC June 19, 2014)..... *passim*

Other Authorities

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009)..... 40, 52, 53

Office of the Director of National Intelligence, *Joint Statement from ODNI and the U.S. DOJ* (Sept. 12, 2014) 12, 19, 37, 38, 62

Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities* (June 26, 2014) 13

Statement by the President on the Section 215 Bulk Metadata Program (March 27, 2014)..... 17, 18, 62

INTRODUCTION

This appeal presents the question whether the Section 215 bulk telephony-metadata program, as authorized by 50 U.S.C. § 1861, is constitutional. Under that anti-terrorism program, the government acquires from certain telecommunications companies business records that contain telephony metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or the content of, the calls. The government does not (and cannot under the court orders establishing the program) use this telephony metadata to compile “rich profile[s] of every citizen.” Pl. Br. 1. Instead, the government, pursuant to Article III judicial authorization and oversight, conducts targeted electronic queries of the bulk telephony metadata in order to uncover links between and among individuals suspected of association with terrorism. The only metadata that government analysts ever review is the tiny fraction of metadata that is responsive to those electronic queries, and the vast bulk of the information is therefore never viewed by anybody.

The district court correctly concluded that the Fourth Amendment permits the government to maintain this valuable counter-terrorism program. Congress authorized the Foreign Intelligence Surveillance Court to issue production orders requiring certain telecommunications companies to produce telephony metadata the companies maintain for their own business purposes. The Fourth Amendment gives Congress broad latitude to require companies to produce business records that are relevant to law-enforcement or national-security investigations, and plaintiff has no Fourth Amendment privacy interest in a company's business records. Nor does plaintiff have a constitutional privacy interest in the telephony metadata itself under the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which held that it is not reasonable for the customers of telecommunications companies to expect that the call-routing information that customers provide to the company will remain private. Contrary to plaintiff's contentions, technological advances since *Smith* have not made a telephone company's records of metadata more private today than comparable records were 35 years ago. Indeed, modern computing technology enables the government to minimize any intrusion on privacy by

carefully controlling and limiting how the metadata is used and disseminated in the service of countering the continuing terrorist threat. The district court's judgment should be affirmed.

STATEMENT OF JURISDICTION

Plaintiff's complaint invoked the district court's jurisdiction under 28 U.S.C. § 1331. ER 123. On June 3, 2014, the district court entered a final judgment granting the government's motion to dismiss and denying plaintiff's motion for a preliminary injunction. ER 11. On July 1, 2014, plaintiff filed a timely notice of appeal. ER 9-10. This Court has appellate jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

Pursuant to authorization from the Foreign Intelligence Surveillance Court under Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861, the government acquires from certain telecommunications companies business records that consist of telephony metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or include the content of, the calls. The government then, pursuant to further individualized judicial

authorization, conducts targeted electronic queries of that information for links between and among suspected-terrorist contacts and other, previously unknown contacts; those links provide valuable information that aids counter-terrorism investigations.

The issues are:

1. Whether plaintiff has standing to challenge the Section 215 program.
2. Whether the district court correctly concluded that the Section 215 program is consistent with the Fourth Amendment.
3. Whether the district court correctly denied plaintiff a preliminary injunction.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes and other authorities are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

I. Nature Of The Case

Plaintiff Anna J. Smith brought this lawsuit in June 2013 challenging the government's Section 215 bulk telephony-metadata program and seeking declaratory and injunctive relief. ER 136. Six months after filing this suit—and four days after another court entered

a preliminary injunction against the Section 215 program, *see Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*, No. 14-5004 (D.C. Cir. Jan. 3, 2014), plaintiff moved for a preliminary injunction. ER 135. The government moved to dismiss. ER 134. The district court granted the government's motion to dismiss and denied plaintiff's motion for a preliminary injunction. ER 8.

Plaintiff filed a notice of appeal from the district court's final judgment about a month later. ER 10. Plaintiff then moved in this Court for expedited briefing and argument, which the Court granted.

II. Statutory Background

At issue in this case is the constitutionality of an important facet of the government's intelligence-gathering capabilities aimed at combating international terrorism—a bulk telephony-metadata program the government operates pursuant to judicial orders and under the authority of the Foreign Intelligence Surveillance Act.

A. Section 215

Congress enacted the Foreign Intelligence Surveillance Act in 1978 to authorize and regulate certain governmental surveillance of communications and other activities conducted to gather foreign

intelligence. The Act created a special Article III court, the Foreign Intelligence Surveillance Court, composed of federal district court judges designated by the Chief Justice, to adjudicate government applications for ex parte orders authorized by the statute. *See* 50 U.S.C. § 1803(a).

Section 501 of the Foreign Intelligence Surveillance Act—which we refer to as “Section 215” because that provision was substantially amended by Section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861—authorizes the government to apply to the Foreign Intelligence Surveillance Court “for an order requiring 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 or clandestine intelligence activities.” 50 U.S.C. § 1861(a)(1). As amended in 2006, Section 215 requires that the application include “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.” *Id.* § 1861(b)(2)(A). Section 215 also includes other requirements that the government must satisfy to obtain a court order

to produce business records or other tangible things. *See, e.g., id.* § 1861(a)(2)(A), (b)(2)(A) (investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 or a successor thereto); *id.* § 1861(b)(2)(B) (application must “enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available” under the order). If the government makes the requisite factual showing, a Foreign Intelligence Surveillance Court judge “shall enter an ex parte order as requested, or as modified, approving the release of tangible things.” *Id.* § 1861(c)(1).

Section 215 establishes a detailed mechanism for judicial review of such orders. The recipient of an order to produce tangible things under Section 215 may challenge the order before another Foreign Intelligence Surveillance Court judge. *See* 50 U.S.C. § 1861(f)(2). Further review is also available in the Foreign Intelligence Surveillance Act Court of Review and, ultimately, in the Supreme Court. *See id.* § 1861(f)(3).

In addition to this system of judicial review, the Foreign Intelligence Surveillance Act requires substantial congressional

oversight of programs operated under Section 215. In particular, the Attorney General must furnish reports detailing activities under the Act to the House and Senate Intelligence and Judiciary Committees. *See* 50 U.S.C. §§ 1808, 1826, 1846. The Act also requires the Attorney General to report all requests made to the Foreign Intelligence Surveillance Court under Section 215 to the House and Senate Intelligence and Judiciary Committees. *See id.* § 1862(a); *see also id.* §§ 1862(b) and (c), 1871(a)(4).

B. The Section 215 Bulk Telephony-Metadata Program

The United States operates a telephony-metadata intelligence-gathering program under Section 215 as part of its efforts to combat international terrorism. Telephony metadata are data about telephone calls, such as the date and time a call was made, what number a telephone called or received a call from, and the duration of a call. SER 9-10; ER 66. Companies that provide telecommunications services create and maintain records containing telephony metadata for the companies' own business purposes, such as billing and fraud prevention, and they provide those business records to the federal government in bulk pursuant to court orders issued under Section 215.

The data obtained under those Foreign Intelligence Surveillance Court orders do not include information about the identities of individuals; the content of the calls; or the name, address, financial information, or cell site locational information of any telephone subscribers. SER 9-10; ER 67.

Under the Section 215 bulk telephony-metadata program, the government consolidates the metadata aggregated from certain telecommunications companies. Although the program operates on a large scale and collects records from multiple telecommunications providers, the Foreign Intelligence Surveillance Court has explained that “production of all call detail records of all persons in the United States has never occurred under this program.” SER 31 n.5. Various details of the program remain classified, precluding further explanation here of its scope, but the absence of those details cannot justify unsupported assumptions. There is no support, for example, for the assumption that the program collects information about “every citizen,” Pl. Br. 1, or about “nearly all calls,” ER 125, or from every telecommunications provider. Nor are those conclusions correct. *See*

Decl. of Teresa H. Shea ¶ 8, *Klayman v. Obama*, No. 13-cv-851 (D.D.C. filed May 9, 2014) (“May 2014 Shea Decl.”).¹

The government uses the Section 215 telephony-metadata program as a tool to facilitate counterterrorism investigations—specifically, to ascertain whether international terrorist organizations are communicating with operatives in the United States. When a selector (the query term), such as a telephone number, is reasonably suspected of being associated with a terrorist organization, government analysts may then, through querying, obtain telephone numbers (or other metadata) that have been in contact within two steps, or “hops,” of the suspected-terrorist selector. *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-96, at 7-8, 12 (FISC June 19, 2014) (“June 19 Primary Order”).² Except in exigent circumstances, the Foreign Intelligence Surveillance Court must approve in advance the government’s use of query terms under that reasonable, articulable suspicion standard. *Id.* at 7-8. This

¹ We explain below that the government should prevail as a matter of law even if the scope of the program were as broad as plaintiff alleges. The May 2014 Shea declaration is included in the Addendum.

² http://www.dni.gov/files/documents/0627/BR%2014-96_Primary_Order.pdf. This document is included in the Addendum.

process enables analysts to identify, among other things, previously unknown contacts of individuals suspected of being associated with terrorist organizations.

The Foreign Intelligence Surveillance Court first authorized the government to obtain business records containing bulk telephony metadata from telecommunications companies under the authority of Section 215 in May 2006. SER 13. The Foreign Intelligence Surveillance Court's authorization of the program is renewed approximately every 90 days. Since May 2006, the Foreign Intelligence Surveillance Court has renewed the program 38 times in court orders issued by seventeen different judges.³ Most recently, the Foreign Intelligence Surveillance Court reauthorized the Section 215 telephony-

³ SER 9, 13; *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-01 (FISC Jan. 3, 2014), available at [http://www.dni.gov/files/documents/BR%2014-01%20Redacted%20Primary%20Order%20\(Final\).pdf](http://www.dni.gov/files/documents/BR%2014-01%20Redacted%20Primary%20Order%20(Final).pdf); *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-67 (FISC Mar. 28, 2014); available at http://www.dni.gov/files/documents/0627/BR_14-67_Primary_Order.pdf; June 19 Primary Order.

metadata program on September 12, 2014, in an order that expires on December 5, 2014.⁴

Section 215 generally requires the government to follow “minimization procedures” governing the use, dissemination, and retention of information obtained under that statute. *See* 50 U.S.C. § 1861(c)(1), (g). Consistent with that requirement, the Foreign Intelligence Surveillance Court orders authorizing the program require the government to implement comprehensive procedures limiting access to and use of the telephony metadata acquired under the program. SER 14-15; *see generally* June 19 Primary Order. Those minimization procedures required by those orders include the restriction that the government may query the database only using a selector for which there is reasonable, articulable suspicion (as determined by a court) that the selector is associated with a foreign terrorist organization

⁴ The Director of National Intelligence declassified the fact of that reauthorization on September 12, 2014. *See* Office of the Director of National Intelligence, *Joint Statement from ODNI and the U.S. DOJ*, (Sept. 12, 2014), *available at* <http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1110-joint-statement-from-the-odni-and-the-u-s-doj-on-the-declassification-of-renewal-of-collection-under-section-501-of-the-fisa>. (“9/12 ODNI-DOJ Joint Statement”).

previously identified to the Foreign Intelligence Surveillance Court as the subject of a counterterrorism investigation. SER 11, 15; June 19 Primary Order 7-8, 12.

The Section 215 bulk telephony-metadata program is not a program of “mass surveillance.” Pl. Br. 1; *see* SER 13-14. On the contrary, the carefully controlled electronic querying process means that the vast majority of the metadata, though in the government’s possession, is never reviewed by any person. SER 12. In 2012, for example, government analysts performed queries using fewer than 300 suspected-terrorist selectors, and the number of records responsive to such queries was a very small percentage of the total volume in the database. SER 12-13. In 2013, the number of suspected-terrorist selectors was only 423.⁵ Under the judicial orders authorizing the program, government analysts may only review telephony metadata within one or two steps of the suspected-terrorist selector. June 19

⁵ Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities* (June 26, 2014), *available at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

Primary Order 7-8, 11-12.⁶ The telephony metadata returned from a query do not include the identities of individuals; the content of any calls; or the name, address, financial information, or cell site locational information of any telephone subscribers or parties to the call, because the metadata obtained under this program do not contain such information. SER 9-10. The Foreign Intelligence Surveillance Court orders also require metadata in the database to be destroyed no later than five years after the information is obtained unless the metadata is subject to a litigation hold. June 19 Primary Order at 13.

The government does not compile comprehensive records or dossiers, even on suspected terrorists, from Section 215 telephony metadata. SER 14. Instead, the government uses the results of specific queries in conjunction with a range of analytical tools to ascertain contact information that may be of use in identifying individuals who may be associated with certain foreign terrorist organizations because they have been in communication with certain suspected-terrorist telephone numbers or other selectors. SER 14. The Foreign

⁶ The first step represents an immediate contact of the suspected-terrorist selector; the second step represents an immediate contact of a first-step contact. SER 12.

Intelligence Surveillance Court's Section 215 orders prohibit the National Security Agency from disseminating to other agencies any information concerning U.S. persons (which includes citizens and lawful permanent residents, *see* 50 U.S.C. § 1801(i)) unless a senior National Security Agency official determines that the information is necessary to understand counterterrorism information or assess its importance.

SER 13-15. The National Security Agency disseminates under the Section 215 program only the tiny fraction of metadata that is associated with suspected-terrorist activity, or are responsive to queries using those suspected-terrorist selectors. SER 15. Subject to those constraints, the result of this analysis provides information the government may use in counter-terrorism investigations.

The program is subject to a rigorous regime of safeguards and oversight, including technical and administrative restrictions on access to the database, internal National Security Agency compliance audits, Department of Justice and Office of the Director of National Intelligence oversight, and reports both to the Foreign Intelligence Surveillance Court and to congressional intelligence committees. SER 16. For example, the Foreign Intelligence Surveillance Court orders

creating the program require the National Security Agency to report to the Foreign Intelligence Surveillance Court the number of instances in which the National Security Agency has shared with other government agencies Section 215 telephony-metadata query results about U.S. persons. June 19 Primary Order 15-16.

The substantial protections in the Section 215 program reflect longstanding minimization requirements imposed by Foreign Intelligence Surveillance Court orders under Section 215, as well as two modifications to the program that were announced by the President in January 2014 and adopted in subsequent Foreign Intelligence Surveillance Court orders. *See* SER 16-17, 102. Prior to those modifications, the Foreign Intelligence Surveillance Court orders establishing the program provided that one of 22 designated officials within the National Security Agency had to determine that a proposed suspected-terrorist selector met the reasonable, articulable suspicion standard. SER 15. Those earlier Foreign Intelligence Surveillance Court orders also permitted the government to obtain query results that revealed metadata up to three steps away from the query selector. SER 12. Under the changes the President announced, which the FISC

subsequently implemented, analyst review of telephony-metadata query results is limited to results within two steps (rather than three) of the suspected-terrorist selector, and there must be an advance judicial finding by the Foreign Intelligence Surveillance Court that the reasonable, articulable suspicion standard is satisfied as to each suspected-terrorist selector used in queries, except in emergency circumstances (in which case the Foreign Intelligence Surveillance Court must retrospectively consider whether to approve the selector). *See In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-01 (FISC Feb. 5, 2014).⁷

On March 27, 2014, the President further announced, after having considered options presented to him by the Intelligence Community and the Attorney General, that he will seek legislation to replace the Section 215 bulk telephony-metadata program. Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), *available at* <http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program> (“3/27 President

⁷ [http://www.dni.gov/files/documents/BR%2014-01%20MTA%20and%20Order%20with%20redactions%20\(Final\).pdf](http://www.dni.gov/files/documents/BR%2014-01%20MTA%20and%20Order%20with%20redactions%20(Final).pdf).

Statement”). The President stated that his goal was to “establish a mechanism to preserve the capabilities we need without the government holding this bulk metadata” so as to “give the public greater confidence that their privacy is appropriately protected, while maintaining the tools our intelligence and law enforcement agencies need to keep us safe.” *Id.* Instead of the government obtaining business records of telephony metadata in bulk, the President proposed that telephony metadata should remain in the hands of telecommunications companies. The President stated that “[l]egislation will be needed to permit the government to obtain this information with the speed and in the manner that will be required to make this approach workable.” *Id.* Under such legislation, the government would be authorized to obtain from companies telephony metadata within two steps of judicially authorized selectors. The President explained that, in the meantime, the government would seek from the Foreign Intelligence Surveillance Court a 90-day reauthorization of the existing Section 215 program, and the Foreign Intelligence Surveillance Court has since then entered three orders reauthorizing the program with the President’s two modifications, most recently on September 12, 2014.

See 9/12 ODNI-DOJ Joint Statement. Absent further legislation, Section 215 will sunset on June 1, 2015. *See* 50 U.S.C. § 1861 note.

III. Proceedings Below

A. This Suit

The Foreign Intelligence Surveillance Court issues two kinds of orders under the Section 215 program: so-called “primary orders” authorizing the government to operate, and setting the general ground rules for, the program for approximately 90-day periods; and “secondary orders” issued to individual telecommunications companies that order them to produce business records containing telephony metadata pursuant to the general authorization of the primary order.

In June 2013, a classified secondary order of the Foreign Intelligence Surveillance Court issued under Section 215 was disclosed publicly in an unauthorized manner. That order required Verizon Business Network Services—and only that entity—to turn over in bulk certain business records of the company containing telephony metadata. SER 115-16. The order expired on July 19, 2013. SER 118. The Director of National Intelligence subsequently confirmed the authenticity of that secondary order. Although the government has

disclosed, in redacted form, some primary orders entered by the Foreign Intelligence Surveillance Court renewing the Section 215 program, it has not disclosed or confirmed the existence of any other secondary order; nor has it revealed the identity of any carrier that participates in the program now, or any entity other than Verizon Business Network Services that has participated in the program in the past. *See* May 2014 Shea Decl. ¶ 8.

Plaintiff Anna J. Smith is an individual who alleges that she is a subscriber of Verizon Wireless. ER 123. Shortly after the June 2013 unauthorized public disclosure of the Verizon Business Network Services secondary order, plaintiff brought this case challenging the lawfulness of the Section 215 bulk telephony-metadata program. ER 136. Her amended complaint alleged that this program violated the First and Fourth Amendments to the Constitution, and exceeded the government's statutory authority. ER 126. She sought declaratory and injunctive relief. ER 126. Plaintiff in district court, however, conceded that her statutory claim and her claim under the First Amendment should be dismissed and does not renew those claims on appeal. *See* Pl. Br. 11 n.14; ER 3.

B. The District Court's Opinion

Six months after filing this suit—and four days after another district court entered a preliminary injunction against the Section 215 program, *see Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*, No. 14-5004 (D.C. Cir. Jan. 3, 2014), plaintiff moved for a preliminary injunction against the Section 215 bulk telephony-metadata program. ER 135. The government moved to dismiss the complaint for lack of jurisdiction and failure to state a claim. ER 134.

The district court granted the government's motion to dismiss and denied plaintiff's motion for a preliminary injunction. ER 8. The court, in a brief footnote, held that plaintiff had standing to challenge the Section 215 program. ER 3 n.2. The court reasoned that the government must have acquired plaintiff's telephony metadata under the Section 215 program because she is a "Verizon customer." *Id.*

The court then rejected plaintiff's argument that the Section 215 program violates the Fourth Amendment. The court found controlling the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), and a number of decisions in this Court holding that individuals have no Fourth Amendment privacy interest in telephony metadata.

ER 5-6. The court also found significant that this case involved telephony metadata contained in the business records of telecommunications companies, and noted that “customers lack a reasonable expectation of privacy in . . . business records” collected by the government from a private company. ER 5. The court noted that the court in the *Klayman* case had reached a contrary conclusion (currently on appeal), but concluded that the reasoning in that case was inconsistent with controlling precedent. ER 8.

SUMMARY OF ARGUMENT

Plaintiff seeks to enjoin the operation of an important government anti-terrorism program that all three branches of government have authorized, including the Foreign Intelligence Surveillance Court on dozens of occasions in orders issued by numerous different Article III judges. Plaintiff characterizes this Section 215 bulk telephony-metadata program as one of “mass surveillance” that involves “surveillance” of “hundreds of millions of people.” Pl. Br. 1, 16. That is inaccurate.

Under the Section 215 program, the government acquires from telecommunications companies business records that contain telephony

metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or include the content of, the calls. The government is prohibited from using, and does not use, the Section 215 database to indiscriminately assemble private details about anyone; indeed, the program is not really a program of “surveillance” at all. It is true that, under the program, the government acquires a large volume of business records containing telephony metadata. But consistent with the governing Foreign Intelligence Surveillance Court orders authorizing the program, that information is used and analyzed only under highly restricted circumstances. The government conducts, pursuant to judicial authorization, targeted queries of certain metadata in that database associated with individuals suspected of ties to terrorism. Records of metadata about the calls of other individuals may be analyzed only in the small fraction of instances in which the metadata in those records are within one or two degrees of contact with another record reasonably suspected of association with terrorism. The vast bulk of the metadata is never viewed by any government analyst.

The district court correctly concluded that the Fourth Amendment permits the government to maintain this carefully tailored and judicially supervised anti-terrorism program, and the judgment below should be affirmed.

1. Plaintiff has not established standing to sue. There is no evidence that the government has collected any business records containing information about plaintiff's calls under the Section 215 telephony-metadata program. Plaintiff states that she is a subscriber of Verizon *Wireless*, but there is no evidence that the government has ever acquired any business records from that company. The only available evidence concerning the identities of the carriers that participate in the program is that a different company—Verizon *Business Network Services*—participated for a few months last year. There is likewise no evidence to support plaintiff's speculation that the government must be collecting all telephone records from Verizon Wireless based on the mere fact that the government has acknowledged that the Section 215 program is broad in scope.

Even if the government has acquired business records containing telephony metadata about plaintiff's calls (and there is no evidence that

it has), plaintiff has not shown how the mere possession of that information by the government would injure her in a legally cognizable way. The carefully limited querying process means that only a small fraction of the Section 215 telephony metadata is actually reviewed by any person. It is speculative whether telephony metadata about plaintiff's calls has been, or would be in the future, among that tiny fraction of information. And plaintiff never explains how she suffers a cognizable Article III injury from the mere presence of inert metadata previously conveyed to her phone company that languishes in a government database unreviewed by any human being.

2. The district court correctly sided with every other federal judge to have decided the question (except the court in *Klayman*) in concluding that the Fourth Amendment permits the government to maintain the Section 215 program. That conclusion follows from *Smith v. Maryland*, 442 U.S. 735 (1979), and cases in this Court applying *Smith*, which hold that individuals lack a Fourth Amendment privacy interest in telephone call record information provided by callers to their telecommunications companies. That reasoning applies with particular force where, as here, plaintiff is claiming a privacy interest in telephony

metadata acquired pursuant to statutory authorization and court orders from the business records of telecommunications companies. The Fourth Amendment gives Congress broad latitude to require companies to produce records for law enforcement or counter-terrorism purposes, and plaintiff has no constitutional privacy interest in the corporate business records of Verizon Wireless.

Contrary to plaintiff's contentions, there is no basis for concluding that changes in technology since *Smith* was decided 35 years ago, or the Supreme Court's decision in *Riley v. California*, 134 S. Ct. 2473 (2014), give her a constitutional privacy interest in Verizon Wireless's business records. Technology has indeed advanced since then, but the type and nature of telephony metadata at issue in this case—as in *Smith*—has not changed materially. And apart from the fact that both cases involve telephones, this case is wholly unlike *Riley*, which involved actual review by police of private information on cellular telephones seized incident to arrests. There is no parallel between those searches and the acquisition of business records of telecommunications companies containing metadata that individuals have conveyed to those companies, only a tiny fraction of which are accessible for review by

government personnel, and then only under highly restricted, judicially supervised conditions. The notion that plaintiff's Fourth Amendment privacy interests have been infringed by the Section 215 program is especially implausible, given that it is speculative whether any government analyst ever has reviewed or would review metadata about plaintiff's calls.

Even if plaintiff had a cognizable privacy interest in Verizon Wireless's business records—and she does not—the Fourth Amendment would permit the government to acquire those records under the special needs doctrine. The Section 215 telephony-metadata program serves the paramount government interest in preventing and disrupting terrorist attacks on the United States, a compelling special governmental need. And because of the significant safeguards in the program—including a requirement of court authorization based on reasonable suspicion before a human analyst accesses the data—the impact on cognizable privacy interests is at most minimal.

3. There is no basis for plaintiff's request for the extraordinary remedy of preliminary injunctive relief. The Section 215 telephony-metadata program serves important national security interests, and

courts are rightly sensitive to the risks of handcuffing the government's efforts to prevent harm to the Nation. Plaintiff claims to suffer irreparable harm from this anti-terrorism program, but waited six months after filing her complaint before seeking preliminary relief. Plaintiff has at most a minimal privacy interest in having metadata about her calls removed from the Section 215 database, one that is outweighed by the public interest in maintaining the program's important capabilities in combating the continuing terrorist threat.

STANDARD OF REVIEW

The district court's decision to grant the government's motion to dismiss is a question of law that the Court reviews de novo.

Entry of a preliminary injunction is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Natural Res. Def. Council*, 555 U.S. 7, 22 (2008). "A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public

interest.” *Id.* at 20; *see also Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131-35 (9th Cir. 2011).

ARGUMENT

I. Plaintiff Lacks Standing To Challenge The Section 215 Bulk Telephony-Metadata Program.

A. To establish Article III standing, a plaintiff must identify an injury that is “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (citations omitted). The “standing inquiry has been especially rigorous when,” as here, a plaintiff urges that “an action taken by one of the other two branches of the Federal Government was unconstitutional,” and where “the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs.” *Id.* (citation and internal quotation marks omitted).

The Supreme Court’s decision in *Amnesty International* is particularly instructive. The plaintiffs in that case were various human-rights, labor, and media organizations who sought to challenge the constitutionality of amendments to the Foreign Intelligence Surveillance Act made in 2008 that expanded the government’s

authority to conduct surveillance of non-U.S. persons located abroad. 133 S. Ct. at 1144. The Court rejected the plaintiffs' speculation that their communications might be subject to surveillance under the authority conferred by those amendments, despite their claim that they communicated with suspected terrorists. The Court noted that the plaintiffs' claimed injury rested on a "speculative chain of possibilities," such as whether the government would target communications to which the plaintiffs were parties and whether the government would succeed in intercepting plaintiffs' communications in doing so. *See id.* at 1148-52.

B. Here, as in *Amnesty International*, plaintiff's claim to injury as a result of the Section 215 program is based only on speculation. Plaintiff claims to suffer ongoing "distress[]" from alleged "monitoring" of information about her calls as a result of the program. ER 125. But that injury could only occur if it were imminently likely that the government would acquire business records containing telephony metadata about her calls. Such an allegation of future injury, as the Supreme Court has "repeatedly reiterated," "must be *certainly impending* to constitute injury in fact"; "[a]llegations of *possible* future

injury’ are not sufficient.” *Amnesty Int’l*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (alteration and emphasis by the Court); see also *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 345 (2006); *Coons v. Lew*, 2014 WL 3866475, at *3 (9th Cir. Aug. 7, 2014).⁸ Plaintiff’s asserted future injury rests on an impermissibly speculative causal chain.

First, plaintiff can only speculate whether the government has ever collected any metadata about her. The only support plaintiff provides for that assumption is the assertion that she is a subscriber of Verizon Wireless. ER 121, 123. But there is no evidence in the record that the government has acquired metadata from Verizon Wireless under the Section 215 program, let alone that it would do so in the imminent future. The government has publicly acknowledged only one Section 215 production order, which was directed to a separate entity, Verizon Business Network Services. SER 115. And there is no evidence

⁸ In some instances, the Supreme Court has “found standing based on a ‘substantial risk’ that the harm will occur.” *Amnesty Int’l*, 133 S. Ct. at 1150 n.5; see, e.g., *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014). But “to the extent that the ‘substantial risk’ standard is relevant and is distinct from the ‘clearly impending’ requirement” in this context, *Amnesty Int’l*, 133 S. Ct. at 1150 n.5, plaintiffs have fallen short of that standard as well.

about what entities the government will acquire information from in the future, which is the relevant inquiry where, as here, a plaintiff seeks prospective relief. *See Mayfield v. United States*, 599 F.3d 964, 970-72 (9th Cir. 2010). The district court elided the important distinction between Verizon Wireless and the separate business entity of Verizon Business Network Services in finding standing simply because plaintiff is a “Verizon customer.” ER 3 n.2.

Plaintiff’s appellate brief does not defend the district court’s reasoning. Instead, plaintiff bases her standing on the speculation that the government must be collecting business records from Verizon Wireless “[b]ecause of the breadth of the program”; because the Section 215 program involves acquiring business records “from multiple providers”; because it involves information that is “aggregated”; and because of statements in the news media. Pl. Br. 36-37. But the fact that the program is “broad,” or that the media thinks it so, does not demonstrate that the government is acquiring records from Verizon Wireless. On the contrary, the program has never encompassed all, or even virtually all, call records and does not do so today. *See* May 2014 Shea Decl. ¶ 8; SER 31 n.5. And contrary to plaintiff’s assertion, it is

not true that “the program’s effectiveness” depends on the government necessarily acquiring business records from Verizon Wireless. Pl. Br. 37. Plaintiff attempts to support that claim by citing various government statements, but the government has said no such thing. *E.g.*, ER 76; *see also* SER 21.⁹ The identities of telecommunications companies that assist with government intelligence-gathering activities remain classified. *See Electronic Frontier Found. v. Dep’t of Justice*, 2014 WL 3945646, at *5-7 (N.D. Cal. Aug. 11, 2014) (rejecting argument that the providers participating in the Section 215 program have been officially acknowledged).

C. Even were there evidence that the government had collected metadata about plaintiff’s telephone calls under the Section 215 program, she still would lack standing. Plaintiff’s claim to injury from the Section 215 program appears to be based on her allegation that the government’s asserted possession of metadata about her calls (of which

⁹ Plaintiff also speculates that the government may have “collected the call records of” unnamed “Verizon Business subscribers with whom Mrs. Smith has been in contact.” Pl. Br. 36-37. Plaintiff identifies no such contacts or persons.

there is no evidence), and potential use of it to “monitor[]” her calls, causes her “distress[.]” ER 125; *see* Pl. Br. 10 n.13.

Plaintiff provides no plausible explanation for how the program could cause that distress. She does not contend that there is any reasonable likelihood that government personnel would actually review metadata about her calls that the government may have acquired under the Section 215 program. That likelihood is particularly remote if “[n]one of her communications relate to international terrorism or clandestine intelligence activities.” Pl Br. 4. Again, information in the Section 215 database is subject to substantial protections and limits on access imposed by orders of the Foreign Intelligence Surveillance Court. Those orders do not permit indiscriminate access to or review of the metadata; instead, there must be an advance judicial finding (or, in cases of emergency, an advance finding by government officials and judicial approval after the fact) that a given selector is suspected of association with terrorism, and only the small fraction of metadata responsive to queries using such suspected-terrorist selectors—that is, within two steps of the judicially approved selector—may be reviewed.

The Supreme Court made clear in *Laird v. Tatum*, 408 U.S. 1, 10-14 (1972), that subjective fears assertedly arising from the mere possession of information by the government do not create standing to challenge a government intelligence-gathering program. In that case, plaintiffs challenged a government surveillance program, claiming that the program caused them harm. The court held that “[a]llegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm.” *Laird*, 408 U.S. at 14. Notably, the Court reached that conclusion even though the plaintiffs in that case had apparently been subject to surveillance. *See id.* at 39 (Brennan, J., dissenting). Plaintiff’s conclusory claim of injury fares no better here: the possibility that inert metadata about plaintiff’s calls may languish unreviewed in the possession of the government does not support her claimed injury.

In district court, plaintiff attempted to fill that gap in her claim to standing, asserting that, if the government had in fact acquired metadata about her calls, she would suffer a cognizable injury each time the government queries the Section 215 database, even if metadata about her calls were never responsive to a query. But queries of Section

215 metadata are performed electronically; a human analyst reviews only metadata that is responsive to an electronic query, and no one reviews nonresponsive information. It is no more an injury for a computer query to rule out particular telephony metadata as unresponsive to a query than it would be for a canine sniff to rule out a piece of luggage as nonresponsive to a drug investigation, *see United States v. Place*, 462 U.S. 696, 707 (1983) (canine sniff of luggage does not violate a reasonable expectation of privacy), or for a chemical test to rule out a particular substance being cocaine, *see United States v. Jacobsen*, 466 U.S. 109, 123 (1984). Where telephony metadata associated with particular calls remains unreviewed and never comes to any human being's attention, there is no invasion of any constitutionally cognizable privacy interests, and no injury to support standing to sue. At the very least, the absence of any such human review would mean that no infringement of a Fourth Amendment privacy interest demonstrably occurred here. *See infra* p. 54-55.

II. The Fourth Amendment Permits The Government To Maintain The Section 215 Program.

A. Plaintiff Has No Fourth Amendment Privacy Interest In Business Records Of Verizon Wireless That Contain Telephony Metadata.

1. The Supreme Court has rejected the premise of plaintiff's Fourth Amendment argument, holding that there is no reasonable expectation of privacy in the telephone numbers a person dials in order to place a telephone call. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the government's recording of the numbers dialed from an individual's home telephone, through the installation of a pen register at a telephone company, is not a search under the Fourth Amendment. *Id.* at 743-44. The district court below correctly sided with every other court to have decided the matter (except for the court in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013))—including numerous decisions of the Foreign Intelligence Surveillance Court as recently as June of this year—in relying on *Smith* to conclude that the acquisition from telecommunications companies of their own business records consisting of bulk telephony metadata is not a Fourth Amendment “search.” See SER 33-36, 77-78 (FISC opinions); 9/12 ODNI-DOJ Joint Statement; see also *In re Application of the FBI*

for an Order Requiring the Production of Tangible Things, Dkt. No. BR-14-01 (FISC Mar. 20, 2014) (“March 2014 FISC Op.”);¹⁰ *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-96 (FISC June 19, 2014);¹¹ *ACLU v. Clapper*, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013); *United States v. Moalin*, 2013 WL 6079518, at *5-8 (S.D. Cal. Nov. 18, 2013).

Smith is based on fundamental Fourth Amendment principles. First, the Supreme Court recognized that, because the government ascertained the numbers dialed from a particular telephone by installing equipment “on telephone company property,” the petitioner there “obviously [could not] claim that his ‘property’ was invaded or that police intruded into a ‘constitutionally protected area.’” *Smith*, 442 U.S. at 741. The Court also contrasted a pen register, which collects numbers dialed, with a listening device that would permit the government to monitor the content of a communication directly. *Id.*

¹⁰ This opinion and order are available at: http://www.dni.gov/files/documents/BR%2014-01_FISC_Opinion_and_Order_March_20_2014.pdf. It is also reproduced in the Addendum to this brief.

¹¹ This opinion is available at: http://www.dni.gov/files/documents/0627/Memorandum_Opinion_in%20BR_14-96.pdf. It is also reproduced in the Addendum to this brief.

(noting that “pen registers do not acquire the *contents* of communications”) (emphasis the Court’s). Thus, the only Fourth Amendment issue in *Smith* was whether a telephone user has a reasonable expectation of privacy in the numbers he dials. Because telephone users convey numbers to the telephone company in order to complete their calls, and because the telephone company can and does routinely record those numbers for its own business purposes, the Court held that any “subjective expectation that the phone numbers [an individual] dialed would remain private . . . is not one that society is prepared to recognize as reasonable.” *Id.* at 743 (internal quotation marks and citation omitted).

In so holding, the *Smith* Court reaffirmed the established principle that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” 442 U.S. at 743-44. Just as “a bank depositor has no legitimate expectation of privacy in financial information voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business,” a telephone user has no reasonable expectation that conveying a telephone number to

the company will protect that number from further disclosure. *Id.* at 744 (internal quotation marks and citation omitted).

The third-party doctrine reaffirmed in *Smith* is well established and creates a readily discernible bright-line rule establishing what is, and is not, protected under the Fourth Amendment. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 564-65 (2009). It would be nearly impossible for government officials to divine on a case-by-case basis whether an individual might have an expectation of privacy in particular information that the person has conveyed to a third party, and the third-party doctrine provides for certainty, which is essential under the Fourth Amendment. *Id.* at 581-86; *see also, e.g., Atwater v. City of Lago Vista*, 532 U.S. 318, 347 (2001).

Indeed, the privacy interests here are even weaker than in *Smith*. This case concerns repeated orders issued by numerous Article III judges pursuant to statutory authorization directing the production of business records maintained by telecommunications companies for their own business purposes. The pen register in *Smith*, by contrast, directly intercepted the transmission of information from a subscriber to a telecommunications company without any judicial or congressional

authorization. *See* 442 U.S. at 737. It has long been established that the Fourth Amendment gives Congress wide discretion to authorize the production of business records by subpoena, even without a judicial order. *See United States v. Golden Valley Electric Ass’n*, 689 F.3d 1108, 1115-16 (9th Cir. 2012); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984); *United States v. Dionisio*, 410 U.S. 1, 13-14 (1973). Because the Section 215 program is based on court orders issued by Article III judges, the constitutionality of the Section 215 program is even more clear. As the Supreme Court has explained, an order by a court to produce records “present[s] no question of actual search and seizure, but raise[s] only the question whether orders of court for the production of specified records have been validly made.” *Okla. Press Publ’g Co. v. Walling*, 327 U.S. 186, 195 (1946). The Foreign Intelligence Surveillance Court has found dozens of times that these production orders are authorized by Section 215 because the telephony metadata in the business records thereby acquired are relevant to authorized counter-terrorism investigations. *See* 50 U.S.C. § 1861(a); SER 46-50 (FISC opinion).¹² Both the statutory scheme under the Foreign

¹² An amicus brief filed by the Center for National Security

Continued on next page.

Intelligence Surveillance Act and the Foreign Intelligence Surveillance Court orders authorizing the program require privacy safeguards as part of the Section 215 program. *See* SER 14-16; June 19 Primary Order at 4-8.

Here, unlike in *Smith* in which there were no restrictions on what the government could do with the information acquired by a pen register, the government may review metadata under the Section 215

Studies argues—contrary to dozens of Foreign Intelligence Surveillance Court orders—that the Section 215 program is unauthorized by statute. The government has addressed that claim where it has been properly raised on appeal, *see* Br. for Defendants-Appellees at 25-37, *ACLU v. Clapper*, No. 14-42 (2d Cir. argued Sept. 2, 2014), but it is not properly before this Court in this appeal because plaintiff in district court conceded that that claim should be dismissed; the district court thus did not address it; and plaintiff has properly not in this Court raised a statutory claim she has abandoned. *See* ER 3, Pl. Br. 11 n.14; *see also, e.g., Golden Gate Restaurant Ass’n v. San Francisco*, 546 F.3d 639, 653 (9th Cir. 2008). As the government has explained, Congress intended the Foreign Intelligence Surveillance Court (and the courts with appellate jurisdiction over that court, including the Supreme Court) to be the exclusive entities responsible for policing compliance with Section 215’s statutory requirements. The Foreign Intelligence Surveillance Court’s repeated orders authorizing the program therefore are fully sufficient to demonstrate that the program is consistent with the will of Congress. *See Klayman*, 957 F. Supp. 2d at 19-23 (accepting the government’s argument that review of production orders in Foreign Intelligence Surveillance Court is the exclusive venue for challenging compliance with Section 215’s statutory requirements); *ACLU*, 959 F. Supp. 2d at 738-42 (same).

program only in extremely restricted circumstances that are not likely to implicate information about plaintiff's calls. The courts should be particularly reluctant to displace that delicate legislative and judicial balance.

In any event, plaintiff has no reasonable expectation of privacy in the corporate business records of Verizon Wireless. "A customer ordinarily lacks 'a reasonable expectation of privacy in an item,' like a business record, 'in which he has no possessory or ownership interest.'" *Golden Valley*, 689 F.3d at 1116 (quoting *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000)). The telephony metadata plaintiff conveyed to Verizon Wireless for incorporation into that company's business records (and for Verizon Wireless to use for its own business purposes) was a "not confidential communication[]," but rather "only information voluntarily conveyed" to that company. *United States v. Miller*, 425 U.S. 435, 442 (1976). Thus, the privacy interests in this case are weaker than in *Smith*, where the telephony metadata was intercepted by the government by a pen register before that information was incorporated into the company's business records. *See* 442 U.S. at 744-45.

2. Plaintiff does not address how she has a privacy interest in business records produced pursuant to congressionally authorized judicial orders. She does, however, argue that she has a privacy interest in telephony metadata, and that *Smith* is distinguishable. Pl. Br. 15-26. Those arguments do not withstand analysis.

First, plaintiff suggests that it “obvious[ly]” makes a difference that “[t]he surveillance in *Smith* continued for three days,” whereas under the Section 215 program the government obtains and retains business records containing telephony metadata over a longer time period. Pl. Br. 16. But the greater time over which metadata may be collected does not validly distinguish *Smith*, which held that individuals lack a privacy interest in *any* of the telephony metadata voluntarily transmitted to a telephone company because the company’s customers “voluntarily convey[] those numbers to the telephone company” and because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *California v. Greenwood*, 486 U.S. 35, 41 (1988) (quoting *Smith*, 442 U.S. at 743-44). That holding did not depend on the number of days the pen register operated, and any other rule would inject needless uncertainty into an

area in which certainty is crucial to enable government personnel to implement these rules in the field. *See, e.g., Atwater*, 532 U.S. at 347.

Nor does the fact that the government retains and aggregates business records containing telephony metadata give plaintiff a Fourth Amendment privacy interest. *Contra* Pl. Br. 16-17. *Smith* was explicit that “[t]he fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference.” 442 U.S. at 745. The Foreign Intelligence Surveillance Court has explained that the third-party disclosure principle “applies regardless of the disclosing person’s assumptions or expectations with respect to what will be done with the information following its disclosure.” March 2014 FISC Op. 15 (quoting *Smith*, 442 U.S. at 744: “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, *even if information is revealed on the assumption that it will be used only for a limited purpose*”) (emphasis the Foreign Intelligence Surveillance Court’s). For example, once an individual engaged in criminal activity discloses information to a government informant, the individual cannot restrict what the

informant may do with the information, because the disclosure vitiates any privacy interest. *See, e.g., Lopez v. United States*, 373 U.S. 427, 438 (1963). The same is true here.

Plaintiff makes much of the fact that *Smith* involved a pen register that captured information about a single person, whereas the Section 215 program involves acquiring business records containing telephony metadata about many persons. Pl. Br. 16-24. Plaintiff overlooks that Fourth Amendment rights “are personal in nature” and therefore she has no standing to invoke the Fourth Amendment rights of others. *Steagald v. United States*, 451 U.S. 204, 219 (1981); *see also, e.g., Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978). Under *Smith*, no caller has a reasonable expectation of privacy in the telephone numbers he dials. The Foreign Intelligence Surveillance Court has correctly recognized that “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*.”

SER 36.

Accordingly, as the Foreign Intelligence Surveillance Court has explained, “the aggregate scope of the collection and the overall size of [the National Security Agency’s] database are immaterial in assessing whether [] any person’s reasonable expectation of privacy has been violated such that a search under the Fourth Amendment has occurred.” March 2014 FISC Op. at 20. The Supreme Court and other courts agree. *See, e.g., Dionisio*, 410 U.S. at 13 (where single subpoena was a reasonable seizure, it was not “rendered unreasonable by the fact that many others were subjected to the same compulsion”); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (rejecting argument that a subpoena was unreasonable under the Fourth Amendment because it “may make available . . . records involving hundreds of innocent people”). Indeed, the Supreme Court has recognized that, in some respects, any Fourth Amendment intrusion effected by large-scale government operations (as in a drunk-driving checkpoint) is less invasive than when government personnel single out individuals as occurred in *Smith*, in which the government acquired telephony metadata about a single individual and used that information to

prosecute him. *See Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 453 (1990); *Delaware v. Prouse*, 440 U.S. 648, 657 (1979).

In arguing that it should make a Fourth Amendment difference that the government is collecting records on a number of people rather than one, plaintiff cites *United States v. Jones*, 132 S. Ct. 945 (2012), and *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. at 945. Pl. Br. 18-19. Those cases, however, each involved investigations that targeted individual criminal defendants, holding, for very different reasons, that those individuals had a personal Fourth Amendment privacy interest in long-term location monitoring by means of a Global Positioning System (GPS) tracking device. And the holding of *Jones* only confirms that plaintiff has no constitutional privacy interest in Verizon Wireless's business records. The opinion for the Court in *Jones* (which was not a "plurality opinion," Pl. Br. 19) reasoned that placement of a GPS tracking device invaded a property interest. *See* 132 S. Ct. at 950-53. Plaintiff ignores that she has no remotely comparable interest in Verizon Wireless's business records.

Plaintiff (Br. 18-19) stresses the alternative rationale for that holding advanced in a concurring opinion in *Jones* and in the D.C. Circuit's opinion in *Maynard*: according to that view, long-term GPS monitoring raises privacy concerns because it enables the government to aggregate private details of an individual's life in a way that "a stranger" observing those movements could not. *Maynard*, 615 F.3d at 560; *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring). But that logic does not apply to telephony metadata acquired under the Section 215 program. As the D.C. Circuit explained in *Maynard*, unlike location information acquired by GPS monitoring, telephony metadata is conveyed by subscribers to telecommunications companies, which then retain that information and incorporate it into their business records. *See* 615 F.3d at 561 (citing *Smith*, 442 U.S. at 742-43). And unlike the GPS information discussed in *Jones*, the telephony metadata at issue here can be used only under the carefully restricted and judicially supervised querying process, and the vast bulk of the information is never seen by any person.

Plaintiff also notes that the pen register in *Smith* captured only "the numbers dialed" whereas the telephony metadata acquired under

the Section 215 program encompasses additional forms of telephony metadata, such as the duration of calls. Pl. Br. 16. As the district court correctly observed, however, ER 5, this Court has rejected that argument, holding that *Smith* extends to other forms of telephony metadata, encompassing general “data about the ‘call origination, length, and time of call.’” *United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009). *Smith* also applies to other forms of metadata, such as e-mail to-from addresses and Internet Protocol addresses. *See United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008). The kinds of metadata collected by the Section 215 program are not materially different.

These holdings undermine plaintiff’s assertion (Br. 20-21) that the march of technology has made *Smith*’s basic holding—that individuals lack a privacy interest in telephony metadata conveyed to a telecommunications company—obsolete or outdated. Technology has indeed advanced, but telephony metadata is not materially different than it was in 1979, as this Court’s decisions in *Reed* and *Forester* recognize. Indeed, the Supreme Court in *Smith* itself made short work of a similar technology-based argument. The defendant in *Smith*

conceded that he would have had no expectation of privacy in his telephony metadata when calls were completed through a human operator, before technology advanced to permit direct dialing. 442 U.S. at 744. The Supreme Court was “not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.” *Id.* at 744-45.

Nothing in the Supreme Court’s recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), Pl. Br. 19-20, supports a different result here. The issue in *Riley* was whether police needed a warrant to search the data on a cell phone incident to an arrest. *See* 134 S. Ct. at 2489-93. The Supreme Court could not have been more explicit that, because *Riley* involved “*searches* incident to an arrest,” the case did “not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.” *Id.* at 2489 n.1 (emphasis the Court’s).

As plaintiff notes, the Supreme Court in *Riley* observed that advances in cell-phone technology has heightened privacy concerns with searching cell phone devices, but those concerns are not present in this case. Advances in technology mean that cell phones now contain

sensitive content, such as photographs, voicemails, and text messages—a veritable “cache of sensitive personal information” that is private. *Id.* at 2490. But this case involves none of that, only telephony metadata. As in 1979, telephony metadata contains no content, and has been voluntarily disclosed by subscribers to their telephone companies. Moreover, the metadata at issue here has been integrated into those companies’ business records, and may be used or analyzed only under carefully restricted and judicially supervised circumstances. Technology indeed “matters,” Pl. Br. 20 (internal quotation marks omitted), but how it matters depends on the context and the function of the legal doctrine in question. And the concerns expressed by the Supreme Court in *Riley* do not apply in this context.

Plaintiff’s suggestion that advances in technology are a one-way ratchet—apparently operating only to increase Fourth Amendment regulation—overlooks that one important function played by the third-party doctrine relied on by *Smith* is to keep the Fourth Amendment “technology neutral.” Kerr, *supra*, 107 Mich. L. Rev. at 580. “Just as the new technologies can bring ‘intimate occurrences of the home’ out in the open,” a commentator has explained, “so can technological change

and the use of third parties take transactions that were out in the open and bring them inside.” *Id.* In that circumstance, the ability of new technology to shield what had previously been public does not alter the protections of the Fourth Amendment, and the third-party doctrine ensures that the line drawn by the Constitution remains appropriately protective of both privacy and security. *See id.* at 574-75. The third-party doctrine thus compensates for the reality that technology enables criminals and terrorists to substitute the use of third-parties and forms of communication (like e-mail) that were previously unknown to facilitate their violent and unlawful ends. Metadata collected under the Section 215 program includes information about the communications patterns of suspected terrorists that, absent the use of that technology, would otherwise in many cases have been readily observable by government officials (for example, whom someone is communicating with, for how long, and when). *Id.* at 575-77, 580-81.¹³ Advances in

¹³ As Professor Kerr notes, 107 Mich. L. Rev. at 581, this rationale reflects and preserves the Supreme Court’s distinction between the fact that a communication has taken place and the content of that communication. Thus, as the Court recognized in *Smith*, 442 U.S. at 741, the third-party doctrine applies to telephony metadata but not necessarily to the content of an intercepted communication.

technology thus only underscore the continuing need for, and vitality of, the third-party doctrine and *Smith's* holding.

Plaintiff also overlooks the fact that technology can also enhance privacy protections. Technology enables the government to minimize any intrusion on any privacy interests by ensuring that the telephony metadata is used only in narrow, judicially approved circumstances. The telephony metadata in the business records collected under the Section 215 program is electronically searched for connections between records reasonably suspected of association with terrorist activity, and only a tiny fraction of the metadata is ever viewed by a person. The metadata is stored in secure networks to which access is strictly limited, and there are both legal prohibitions and technological controls that prevent even authorized government analysts from indiscriminately searching the telephony metadata absent judicial approval of a selector. *See* SER 14-15.

Given these protections, plaintiff's focus on the possibility that metadata could "reflect[] a wealth of detail" about her or other individuals, Pl. Br. 23 (internal quotation marks omitted), is misplaced. As plaintiff notes, it is only the "result of its queries" to which the

government may apply its analytic tradecraft under the Section 215 program. Pl. Br. 6 n.6. It is most unlikely that the Section 215 program has revealed anything about plaintiff, because the program is directed at identifying terrorist connections, and there is no allegation or evidence that metadata about her calls (even if the government acquired that information) has been among the tiny fraction of metadata reviewed by government personnel after querying. That alone means that no Fourth Amendment “search” demonstrably happened here, and again plaintiff cannot assert the Fourth Amendment privacy interests of others. *See, e.g., Carter*, 525 U.S. at 88; *Place*, 462 U.S. at 707; *Jacobsen*, 466 U.S. at 123.

While in theory bulk telephony-metadata could be used to reveal information about other individuals indiscriminately, that does not, and cannot consistent with the governing Foreign Intelligence Surveillance Court orders, happen under the Section 215 program. Again, use and dissemination of the metadata is carefully controlled, and the government does not use it to assemble information about individuals indiscriminately. The Court must analyze the program as it is—and as the governing Foreign Intelligence Surveillance Court orders require it

to be—not as plaintiff speculates the program could be misused. *Cf. Laird*, 408 U.S. at 11 (noting that speculation that the government might “in the future take some other and additional action detrimental to” them is not a basis for challenging a surveillance program).

In any event, it is true, but beside the point, that telephony metadata acquired under the Section 215 program can be revealing—indeed, the Section 215 program is important precisely because targeted and limited queries of telephony metadata collected in bulk shed light on connections between individuals suspected of association with terrorism and other known and unknown persons. But other business records also can reveal personal information: records of dialed telephone numbers can prove that an individual has been making obscene and harassing phone calls, *see Smith*, 442 U.S. at 737, and checks, deposit slips, and other customer bank records can show significant commercial and personal transactions, *see United States v. Miller*, 425 U.S. at 442-44. Similarly, confessions made to a government informant can provide important information about criminal activity. *See Lopez*, 373 U.S. at 438. The Supreme Court understood those consequences perfectly well, *see Smith*, 442 U.S. at

747-48 (Stewart, J., dissenting); *id.* at 750 (Brennan, J., dissenting); *see also Miller*, 425 U.S. at 451 (Brennan, J., dissenting), yet applied the third-party doctrine to hold that there is no Fourth Amendment privacy interest in any such information. The question is not whether telephony metadata can reveal personal information, but whether it is reasonable to expect that routing information about phone calls will be kept private, even after a customer conveys that information to a telephone company for incorporation into that company's business records and for use by that company to advance its own business purposes. Under *Smith*, the answer to that question is no.

3. Plaintiff cites a number of cases for the idea that “the ‘third party’ rule does not operate like an on-off switch” and that “the mere fact that a person entrusts information to a third party does not necessarily mean that she has surrendered her constitutional right to privacy in the information.” Pl. Br. 24-25. Many of the cases plaintiff cites did not even involve something turned over to a third party, and none remotely shows that an individual has a Fourth Amendment privacy interest in the business records of a private company. Plaintiff, for example, relies on *United States v. Young*, 573 F.3d 711, 716-17 (9th

Cir. 2009), which recognized an individual's expectation of privacy in his hotel room, but this case is much more like *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000), which held that an individual has no reasonable expectation of privacy in information voluntarily conveyed by a person and incorporated into the registration records of a motel.

Plaintiff is also wide of the mark in relying on cases involving the compelled disclosure of the contents of communications, such as e-mail. Pl. Br. 25. Both *Smith* and this Court have explicitly distinguished telephony metadata conveyed to a telephone company (which is at issue here) from “the *contents* of communications” (which is not), in holding that there is no reasonable expectation of privacy in metadata provided to the company. 442 U.S. at 741 (emphasis the Court's); see *Forrester*, 512 F.3d at 510-11. In addition, e-mails are “communications between two subscribers, not communications between the service provider and a subscriber that would qualify as business records.” *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 611 (5th Cir. 2013). This case does not present the question whether the third-party doctrine would apply to the content of communications voluntarily

transmitted to third-parties and not incorporated into the business records of those parties.¹⁴

Justice Alito's concurring opinion in *Jones*, in noting the difficulties and ambiguities of appropriately defining privacy protections in the Digital Age, observed that "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." 132 S. Ct. at 964. The Section 215 program, which the Foreign Intelligence Surveillance Court has repeatedly held is authorized by statute, and which Congress was aware of when it reauthorized Section 215 in 2009 and 2011, *see* SER 105-14, reflects that kind of judgment. In authorizing the government to acquire telephony metadata in bulk in order to combat terrorism, Congress provided for supervision of the process by the Foreign Intelligence Surveillance Court, and was careful

¹⁴ Plaintiff cites (Br. at 25-26) the Eleventh Circuit's opinion in *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), which held that the collection of cell-site data can implicate a Fourth Amendment privacy interest. The Eleventh Circuit has vacated that opinion upon granting rehearing en banc. *See* No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). Cell-site locational data is not among the telephony metadata acquired under the Section 215 program, SER 9-10, and plaintiff disavows any argument based on the collection of location information, *see* Pl. Br. 12 n.15.

to require privacy protections through the imposition of minimization procedures limiting the government's use of the information. *See* 50 U.S.C. § 1861(b)(2), (c)(1), (g). The political branches continue to debate the best means of accomplishing the Section 215 program's goals, but this Court should not lightly conclude that this program infringes a Fourth Amendment privacy interest where Congress, under current law, has already balanced the relevant interests.

B. If Obtaining Metadata Implicated A Fourth Amendment Privacy Interest, The Program Would Still Be Constitutional

Even if obtaining bulk telephony metadata from the business records of telecommunications companies were a Fourth Amendment “search,” it would nevertheless be constitutionally permissible. The Fourth Amendment bars only unreasonable searches and seizures, and the Section 215 telephony-metadata program is reasonable under the standard applicable to searches that serve “special needs” of the government. *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). The national security and safety interests served by the Section 215 program are special needs of the utmost importance that go beyond ordinary law enforcement needs. *See Nat'l Treasury Emps.*

Union v. Von Raab, 489 U.S. 656, 674 (1989) (noting “national security” interest in deterring drug use among Customs Service employees); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322-23 (1972); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006); *MacWade v. Kelly*, 460 F.3d 260, 270-71 (2d Cir. 2006) (citing *Sitz*, 496 U.S. at 444).

Plaintiff agrees that the special-needs doctrine applies where compliance with “the warrant and probable-cause requirements” is “impracticable.” Pl. Br. 29. That standard governs here because, as the government has shown and the Foreign Intelligence Surveillance Court has repeatedly concluded, the Section 215 bulk telephony-metadata program provides an efficient means to identify otherwise-unknown associations (within one or two steps of contact) with telephone numbers and other selectors that are reasonably suspected of being used by terrorist organizations. The bulk collection of metadata allows the government to identify connections using retrospective analysis of calls that occurred before the relevant terrorist connection became known. The Foreign Intelligence Surveillance Court orders authorizing the Section 215 bulk telephony-metadata program permit the government to retain a historical repository of up to five years’ worth of

telephony metadata, cutting across multiple providers, for intelligence analysis purposes that could not be accomplished as effectively, if at all, with more targeted investigative tools, such as probable-cause warrants. SER 20-26, ER 74-76. Under current law, “serving the phone companies with demands for records relating to particular terrorism suspects,” Pl. Br. 34, does not allow the historical analysis conducted under the Section 215 program to occur as effectively. SER 25.

Although, as plaintiff notes, Pl. Br. 29-30, the President has proposed legislation to accomplish the Section 215 program’s goal through other means, those means would not merely substitute for probable-cause warrants, but would instead require new legislation, which Congress is now considering. *See* 9/12 ODNI-DOJ Joint Statement.¹⁵ In the meantime, the President has also stressed the “importance of maintaining this capability,” 3/27 President Statement, and has authorized the government to continue the program (and the Foreign Intelligence Surveillance Court has continued to issue orders

¹⁵ Legislation reauthorizing the government’s intelligence activities under Section 215 must be enacted, in some form, or the statute will expire on June 1, 2015. *See* 50 U.S.C. § 1861 note.

authorizing the program, most recently on September 12, 2014). The political branches continue to debate the best means of accomplishing the goals of the program, but that is no basis for concluding that the program serves no important function under current law.

Plaintiff's insistence that the government cannot obtain telephony metadata under Section 215 without a warrant and individualized probable cause is particularly anomalous given the broad discretion the Fourth Amendment ordinarily provides the government to compel the production of documents under statutory authorization. Notably, grand jury subpoenas and administrative subpoenas, which do not require warrants or probable cause, have repeatedly been upheld under the Fourth Amendment. *See, e.g., Golden Valley*, 689 F.3d at 1115-16. Section 215 production orders include privacy protections beyond those in administrative subpoenas and grand jury subpoenas, since Section 215 production orders are issued by Article III courts, and the information acquired may be used and disseminated only in accordance with minimization procedures set, supervised, and enforced by the Foreign Intelligence Surveillance Court.

In light of the imperative national-security interests the program serves and the numerous privacy protections that the statute and the Foreign Intelligence Surveillance Court require the government to observe, the program is reasonable under the Fourth Amendment. *See* U.S. Const. amend. IV. That reasonableness standard requires balancing “the promotion of legitimate governmental interests against the degree to which [any search] intrudes upon an individual’s privacy.” *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (citation and internal quotation marks omitted). The interest in preventing terrorist attacks by identifying and tracking terrorist operatives is a national security concern of compelling importance. *See Haig v. Agee*, 453 U.S. 280, 307 (1981) (“no governmental interest is more compelling” than national security); *In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) (“the relevant governmental interest—the interest in national security—is of the highest order of magnitude”). The Section 215 bulk telephony-metadata program enhances the government’s ability to uncover and monitor known and unknown terrorist operatives who could otherwise elude detection, and has meaningfully contributed to counterterrorism investigations. SER 20-26, ER 74-76.

Any Fourth Amendment privacy interest implicated by the Section 215 program, in contrast, is minimal. The governing Foreign Intelligence Surveillance Court orders strictly limit review and analysis of the metadata, and there is no nonspeculative basis to believe that any information concerning plaintiff's calls—or those of the vast bulk of other telephone subscribers—has been or will ever be seen by any person. *See King*, 133 S. Ct. at 1979-80 (finding no Fourth Amendment violation where safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Bd. of Educ. v. Earls*, 536 U.S. 822, 833-34 (2002) (no Fourth Amendment violation where restrictions on access to drug testing results lessened intrusion on privacy); *Vernonia Sch. Dist.*, 515 U.S. at 658 (no Fourth Amendment violation where student athletes' urine was tested for illegal drugs and not for any medical condition); *Sitz*, 496 U.S. at 450-51 (no Fourth Amendment violation where safety interests served by drunk-driving checkpoints outweighed motorists' interests in driving without being stopped). The government obtains telephony metadata in bulk to preserve the information for future analysis based on a reasonable, articulable suspicion; the information is then only accessed

as part of the highly restricted querying process, which requires judicial approval.

Plaintiff asks the government to show more, claiming that the program is an unconstitutional means of serving the paramount need of preventing terrorist attacks because the government has not “describe[d] a single instance” in which the program has “actually stopped an imminent attack” or “aided . . . in achieving any objective that was time-sensitive in nature.” Pl. Br. 33 (quoting *Klayman*, 957 F. Supp. 2d. at 40). The Constitution does not require an anti-terrorism program to have demonstrably prevented a specific terrorist attack to be reasonable. *See Von Raab*, 489 U.S. at 676 n.3 (“a demonstration of danger as to any particular airport or airline” is not required since “[i]t is sufficient that the Government have a compelling interest in preventing an otherwise pervasive societal problem from spreading”); *Cassidy*, 471 F.3d at 84-85; *MacWade*, 460 F.3d at 272. Nor is it problematic that the Section 215 program is only “one means” among many government programs that work together to accomplish the paramount goal of countering terrorism. Pl. Br. 35. To protect the Nation, the government employs a range of counter-terrorism tools and

investigative methods in concert, which often serve different functions in order to complement one another in the service of achieving the overarching goal of preventing attacks. Those tools rarely, however, operate in isolation, and nothing in the Fourth Amendment's special-needs jurisprudence requires a showing that any single program is essential or itself prevented a particular attack. The government has provided examples in which the Section 215 program provided timely and valuable assistance to ongoing counter-terrorism investigations. *See* ER 74-75.

Plaintiff is of the view that there are alternative, "less-intrusive" means of accomplishing the Section 215 program's goals. Pl. Br. 14, 33-35. But the Supreme Court "has 'repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment.'" *City of Ontario v. Quon*, 560 U.S. 746, 763 (2010). The relevant legal standard under the special-needs doctrine is not, as plaintiff seems to think, whether the program is indispensable to counter-terrorism efforts. The standard is whether the program is at least a "reasonably effective means" of advancing the government's paramount interest in preventing terrorism. *Earls*, 536 U.S. at 837.

(quoting *Vernonia*, 515 U.S. at 663). The declarations in the record establish that the Section 215 bulk telephony-metadata program enhances the government’s ability to uncover and monitor known and unknown terrorist operatives who could otherwise elude detection. SER 20-26, ER 74-76. The courts owe deference to the assessment by the Executive Branch—which daily confronts threats to our national security and must make difficult judgments on how best to eliminate those threats—not to plaintiff’s contrary views. *See, e.g., Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2727 (2010); *cf. Sitz*, 496 U.S. at 453-54 (courts should not second-guess “politically accountable officials” on “which among reasonable alternative law enforcement techniques should be employed to deal with a serious public danger”). The program is reasonable under the Fourth Amendment’s special-needs doctrine.

III. There Is No Basis For Entering A Preliminary Injunction.

There is no basis for plaintiff’s alternative request for the Court to enter the extraordinary remedy of preliminary injunctive relief.

“A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer

irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.” *Winter v. Natural Res. Def. Council*, 555 U.S. 7, 20 (2008).

None of those elements has been remotely satisfied here. The Fourth Amendment permits the government to maintain the program.

Plaintiff has not shown she has suffered any harm from the program, let alone irreparable harm—as is underscored by the fact that plaintiff did not move for a preliminary injunction until six months after she filed her lawsuit. ER 135-36.

The balance of equities and the public interest also tip markedly in the government’s favor. Any privacy interest plaintiff has at stake here is surely minimal, particularly given the remote likelihood that metadata pertaining to her calls would ever be reviewed by a human analyst. On the other side of the ledger, the government has a substantial interest in continuing the Section 215 program, a valuable program in the government’s antiterrorism arsenal, for reasons already explained.

In addition, the declarations in the record establish that a preliminary injunction against the program, even one limited to

telephony metadata about plaintiff, would be burdensome. It would require the government to develop a new capability to segregate metadata associated with plaintiff's call records from the rest of the information, and remove that metadata from each new batch of metadata received on a daily basis (assuming the government received any in the first place). SER 27. Those tasks could consume considerable resources, and any technological solution could degrade the program's overall effectiveness by eliminating or cutting off potential call chains that might otherwise reveal connections between individuals associated with terrorist activity. SER 27. Moreover, requiring the government to refrain from collecting and to destroy records regarding plaintiff's calls, as her motion for a preliminary injunction requests, SER 2, would be irreversible, and hence is improper preliminary injunctive relief, because it would grant plaintiff full relief on the merits prematurely. *See Dorfmann v. Boozer*, 414 F.2d 1168, 1173 n.13 (D.C. Cir. 1969).

CONCLUSION

The district court's judgment should be affirmed.

Respectfully submitted,

JOYCE R. BRANDA
*Acting Assistant Attorney
General*

WENDY J. OLSON
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III

/s/ Henry C. Whitaker
HENRY C. WHITAKER
*(202) 514-3180
Attorneys, Appellate Staff
Civil Division, Room 7256
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530*

OCTOBER 2014

**CERTIFICATE OF COMPLIANCE WITH
FEDERAL RULE OF APPELLATE PROCEDURE 32(A)**

I hereby certify that that this brief complies with the requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in 14-point Century Schoolbook, a proportionally spaced font.

I further certify that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 13,119 words excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Henry C. Whitaker
HENRY C. WHITAKER

STATEMENT OF RELATED CASES

The government is aware of no related cases other than the one identified in plaintiff's statement.

/s/ Henry C. Whitaker
HENRY C. WHITAKER

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2014, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. I further certify that I will cause paper copies of this brief to be filed as directed by the Court.

/s/ Henry C. Whitaker
HENRY C. WHITAKER

ADDENDUM

TABLE OF CONTENTS

	<u>Page</u>
50 U.S.C. § 1861.....	A1
Memorandum Opinion in re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things (Foreign Intelligence Surveillance Court – June 19, 2014).....	A8
Primary Order Granting Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things (Foreign Intelligence Surveillance Court – June 19, 2014).....	A21
Opinion and Order Denying Petition to Vacate or Modify Second Order Issued January 3, 2014 (Foreign Intelligence Surveillance Court – March 20, 2014).....	A38
Declaration of Teresa H. Shea, Signals Intelligence Director, (National Security Agency – May 2014)	A69



Effective: March 9, 2006

United States Code Annotated [Currentness](#)

Title 50. War and National Defense ([Refs & Annos](#))

▢ [Chapter 36](#). Foreign Intelligence Surveillance ([Refs & Annos](#))

▢ [Subchapter IV](#). Access to Certain Business Records for Foreign Intelligence Purposes

→→ **§ 1861. Access to certain business records for foreign intelligence and international terrorism investigations**

(a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring 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 or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under [Executive Order 12333](#) (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section

(1) shall be made to--

(A) a judge of the court established by [section 1803\(a\)](#) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include--

(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the 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; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) of this section that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) of this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) of this section be followed.

(2) An order under this subsection--

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d) of this section;

(D) may only require the production of a tangible thing if such 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; and

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a) of this section.

(d)(1) No person shall disclose to any other person that the Federal bureau of investigation has sought or obtained tangible things pursuant to an order under this section, other than to

(A) those persons to whom disclosure is necessary to comply with such order;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f)(1) In this subsection--

(A) the term “production order” means an order to produce any tangible thing under this section; and

(B) the term “nondisclosure order” means an order imposed under subsection (d) of this section.

(2)(A)(i) A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by [section 1803\(e\)\(1\)](#) of this title. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by [section 1803\(e\)\(1\)](#) of this title.

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by [section 1803\(e\)\(1\)](#) of this title. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under [section 1803\(e\)\(2\)](#) of this title.

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection

shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under [section 1803\(b\)](#) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) Minimization procedures

(1) In general

Not later than 180 days after March 9, 2006, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this subchapter.

(2) Defined

In this section, the term “minimization procedures” means--

(A) 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;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [section 1801\(e\)\(1\)](#) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(h) Use of information

Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g) of this section. No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

CREDIT(S)

(Pub.L. 95-511, Title V, § 501, as added Pub.L. 107-56, Title II, § 215, Oct. 26, 2001, 115 Stat. 287; amended Pub.L. 107-108, Title III, § 314(a)(6), Dec. 28, 2001, 115 Stat. 1402; Pub.L. 109-177, Title I, § 106(a) to (e), (f)(2), (g), Mar. 9, 2006, 120 Stat. 196 to 198; Pub.L. 109-178, §§ 3, 4(a), Mar. 9, 2006, 120 Stat. 278, 280.)

AMENDMENT OF SECTION

<Pub.L. 109-177, Title I, § 102(b), Mar. 9, 2006, 120 Stat. 195, as amended Pub.L. 111-118, Div. B, § 1004(a), Dec. 19, 2009, 123 Stat. 3470; Pub.L. 111-141, § 1(a), Feb. 27, 2010, 124 Stat. 37; Pub.L. 112-3, § 2(a), Feb. 25, 2011, 125 Stat. 5; Pub.L. 112-14, § 2(a), May 26, 2011, 125 Stat. 216, provided that, effective June 1, 2015, with certain exceptions, this section is amended to read as it read on October 25, 2001. See Sunset Provisions note set out under this section. On October 25, 2001, this section read as follows:>

<§ 1861. Definitions>

<As used in this subchapter [50 U.S.C.A. § 1861 et seq.]:>

<(1) The terms “foreign power”, “agent of a foreign power”, “foreign intelligence information”, “international terrorism”, and “Attorney General” shall have the same meanings as in section 1801 of this title.>

<(2) The term “common carrier” means any person or entity transporting people or property by land, rail, water, or air for compensation.>

<(3) The term “physical storage facility” means any business or entity that provides space for the storage of goods or materials, or services related to the storage of goods or materials, to the public or any segment thereof.>

<(4) The term “public accommodation facility” means any inn, hotel, motel, or other establishment that provides lodging to transient guests.>

<(5) The term “vehicle rental facility” means any person or entity that provides vehicles for rent, lease, loan, or other similar use to the public or any segment thereof.>

Current through P.L. 113-120 approved 6-10-14

Westlaw. (C) 2014 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT

Declassified by the DNI June 27, 2014

~~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 14-96

MEMORANDUM OPINION

The Court has today issued the Primary Order appended hereto granting the
"Application of the Federal Bureau of Investigation for an Order Requiring the

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

Declassified by the DNI June 27, 2014

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

Production of Tangible Things" ("Application" or "the instant Application"), which was submitted to the Court on June 19, 2014, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. §1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk ("bulk telephony metadata").

On August 29, 2013, Judge Claire V. Eagan of this Court issued an Amended Memorandum Opinion in Docket Number BR 13-109, offering sound reasons for authorizing an application for orders requiring the production of bulk telephony metadata ("August 29 Opinion"). On September 17, 2013, following a declassification review by the Executive Branch, the Court published its redacted August 29 Opinion and the Primary Order issued in Docket Number BR 13-109. On October 11, 2013, Judge Mary A. McLaughlin of this Court granted the FBI's application to renew the authorities approved in Docket Number BR 13-109, issued a Memorandum adopting Judge Eagan's statutory and constitutional analyses, and provided additional analysis on whether the production of bulk telephony metadata violates the Fourth Amendment ("October 11 Opinion"). Both judges of this Court held that the compelled production of such records does not constitute a search under the Fourth Amendment. Judge

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

Declassified by the DNI June 27, 2014

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

McLaughlin further found that the Supreme Court's decision in United v. Jones, ___ U.S. ___, 132 S. Ct. 945 (2012) neither mandates nor supports a different conclusion.

Following a declassification review by the Executive Branch, the Court published the October 11 Opinion and the Primary Order issued in Docket Number BR 13-158 in redacted form a week later on October 18, 2013. Since the date of Judge McLaughlin's re-authorization of the bulk telephony metadata collection in Docket Number BR 13-158, the government has sought on three occasions renewed authority for this collection. The Court has approved those applications in Docket Numbers BR 14-01 (on January 3, 2014), BR 14-67 (on March 28, 2014), and the instant Application.

In approving the instant Application, I fully agree with and adopt the constitutional and statutory analyses contained in the August 29 Opinion and the October 11 Memorandum. In particular, with respect to the constitutional analysis, I concur with Judges Eagan and McLaughlin that under the controlling precedent of *Smith v. Maryland*, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. With respect to the statutory requirements for the issuance of orders for the collection of bulk telephony metadata, I adopt the analysis put forth by Judge Eagan in her August 29 Opinion, and in particular, I note her discussion on the issue of relevance:

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

Declassified by the DNI June 27, 2014

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

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 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. [. . .] 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.

August 29 Opinion at 22-23.

Since the issuance of the August 29 Opinion and October 11 Memorandum, there have been changes to the minimization procedures applied to the bulk telephony metadata collection. These were requested by the government and approved by this Court. Moreover, the legality of the bulk telephony metadata collection has been challenged in litigation throughout the country and considered by four U.S. District

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

Declassified by the DNI June 27, 2014

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

Court judges. Lastly, on December 18, 2013, in an order entered in BR 13-158, Judge McLaughlin granted leave to the Center for National Security Studies ("the Center") to file an *amicus curiae* brief on why 50 U.S.C. §1861 does not authorize the collection of telephony metadata records in bulk. The Center filed its *amicus* brief on April 3, 2014, after the most recent authorization of this collection in Docket Number BR 14-67. Prior to making a decision to grant the instant Application, I considered each of these developments, which I briefly note below.

Changes to Minimization Procedures

Pursuant to 50 U.S.C. §1861(g), the bulk telephony metadata collected pursuant to orders granting the instant Application, as well as all predecessor applications, are subject to minimization procedures. The statutory requirements for minimization procedures under 50 U.S.C. §1861(g) are discussed in the August 29 Opinion. August 29 Opinion at 11. On February 5, 2014, the Court granted the government's Motion for Amendment to Primary Order in Docket Number BR 14-01, which amended the minimization procedures required by the Primary Order in that case in two significant respects. First, the amended procedures preclude the government (except in emergency circumstances) from querying the bulk telephony metadata without first having

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

Declassified by the DNI June 27, 2014

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

obtained, by motion, a determination from this Court that reasonable, articulable suspicion (RAS) exists to believe that the selection term (e.g., a telephone number) to be used for querying is associated with an international terrorist organization named in the Primary Order requiring the production of the bulk telephony metadata.¹ Second, the amended procedures require that queries of the bulk telephony metadata be limited so as to identify only that metadata found within two "hops" of an approved selection term.² The government has requested, and the Court has approved, the same limitations in orders accompanying the two subsequent applications for this collection filed with this Court (i.e., Docket Number BR 14-67 and the instant Application).

On February 25, 2014, the government filed a Motion for Second Amendment to Primary Order in Docket Number BR 14-01, through which it sought further to modify the minimization procedures ("February 25 Motion"). Specifically, the government sought relief from the requirement that it destroy bulk telephony metadata after five

¹ Previously, the minimization procedures allowed for this RAS determination to be made by one of a limited set of high-ranking NSA personnel.

² The first "hop" would include metadata associated with the set of numbers directly in contact with the approved selection term, and the second "hop" would include metadata associated with the set of numbers directly in contact with the first "hop" numbers. Previously, the minimization procedures allowed the government to query the bulk telephony metadata to identify metadata within three "hops" of an approved selection term.

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

Declassified by the DNI June 27, 2014

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

years, based on the government's common law preservation obligations in pending civil litigation. In seeking relief from the five-year destruction requirement, the government proposed a number of additional restrictions on access to and use of the data, all designed to ensure that collected metadata that was more than five years old could only be used for the relevant civil litigation purposes. Although this Court initially denied the February 25 Motion without prejudice, the Court granted a second motion for the same relief on March 12, 2014 ("March 12 Order and Opinion"), that the government sought in order to comply with a preservation order that had been issued by the U.S. District Court for the Northern District of California after this Court's denial of the February 25 Motion. The March 12 Order and Opinion required that the bulk telephony metadata otherwise required to be destroyed under the five year limitation on retention be preserved and/or stored "[p]ending resolution of the preservation issues raised . . . before the United States District Court for the Northern District of California[.]" March 12 Opinion and Order at 6. The March 12 Order and Opinion prohibited NSA intelligence analysts from accessing or using such data for any purpose; permitted NSA personnel to access the data only for the purpose of ensuring continued compliance with the government's preservation obligations; and prohibited any further accesses of BR metadata for civil litigation purposes without prior written notice to this Court. *Id.*

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

Declassified by the DNI June 27, 2014

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

at 6-7. Finally, the March 12 Opinion and Order required the government promptly to notify this Court of any additional material developments in civil litigation pertaining to the BR metadata, including the resolution of the preservation issues in the proceedings in the Northern District of California. *Id.* at 7. The preservation issues raised in the Northern District of California have not yet been resolved. As a result, the government has requested and the Court has approved the same exemption from the five year limitation on retention, subject to the same restrictions on access and use, in Docket Number BR 14-67 and the instant Application.

Prior to deciding whether to re-authorize the bulk telephony metadata collection through the appended Primary Order, I considered with care the stated changes to the minimization procedures. As described, the first set of changes approved in the February 5 Order provide enhanced protections for the bulk telephony metadata. While the March 12 Opinion and Order allows the government to retain bulk telephony metadata beyond five years, it allows the government to do so for the sole purpose of meeting preservation obligations in civil litigation pending against it.

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

Declassified by the DNI June 27, 2014

~~TOP SECRET//SI//NOFORN~~*U.S. District Court Cases*

In recent months, the legality of the bulk telephony metadata collection has been challenged on both statutory and constitutional grounds in proceedings throughout the country, and four U.S. District Court judges have issued opinions on these challenges.

Smith v. Obama, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014);

A.C.L.U. v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *Klayman v. Obama*, 957 F. Supp.

2d 1 (D.D.C. 2013); and *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal.

November 18, 2013). In three of the four cases in which judges have issued opinions

(i.e., all but the *Klayman* case), they have rejected plaintiffs' challenges to this collection.

In particular, with respect to Fourth Amendment challenges raised by plaintiffs, the

judges in *Smith*, *Clapper* and *Moalin* recognized that the Supreme Court's decision in

Smith v. Maryland is controlling and does not support a finding that the bulk telephony

metadata collection is a violation of the Fourth Amendment.

In *Klayman*, Judge Richard J. Leon of the U.S. District Court for the District of

Columbia alone held that the plaintiffs were likely to succeed on their claim that the

bulk telephony metadata collection was an unreasonable search under the Fourth

Amendment. *Klayman*, 957 F. Supp. 2d at 41. Judge Leon ordered the government to

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

Declassified by the DNI June 27, 2014

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

cease collection of any telephony metadata associated with [the plaintiffs'] personal Verizon accounts" and destroy any such metadata in its possession, but he stayed the order pending appeal. *Id.* at 43.

On January 22, 2014, a recipient of a production order in Docket Number BR 14-01 filed a Petition ("January 22 Petition") pursuant to 50 U.S.C. § 1861(f)(2)(A) and Rule 33 of the Foreign Intelligence Surveillance Court ("FISC") Rules of Procedure, asking this Court "to vacate, modify, or reaffirm" the production order issued to it.³ According to the Petitioner, the Petition arose "entirely from the effect on [the recipient] of Judge Leon's Memorandum [Opinion]," and specifically, that Judge's conclusion that the Supreme Court's decision in *Smith v. Maryland* is "inapplicable to the specific activities mandated by the [Section] 1861 order at issue in the *Klayman* litigation." January 22 Petition at 3-4. Pursuant to the requirements of 50 U.S.C. § 1861(f), Judge Rosemary M. Collyer of this Court issued an Opinion and Order on March 20, 2014 ("March 20 Opinion and Order"), finding that the Petition provided no basis for vacating or

³ Following a declassification review by the Executive Branch, the Court published the January 22 Petition filed in Docket Number BR 14-01 in redacted form on April 25, 2014.

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

Declassified by the DNI June 27, 2014

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

modifying the relevant production order issued in Docket Number BR 14-01.⁴ In her March 20 Opinion and Order, Judge Collyer engaged in an extensive analysis of Judge Leon's opinion in *Klayman*, ultimately disagreeing with his conclusion that *Smith v. Maryland* is inapplicable to the collection of bulk telephony metadata.

In issuing the Primary Order appended hereto which re-authorizes the bulk telephony metadata collection, I have carefully examined the noted U.S. District Court opinions, and I agree with Judge Collyer's analysis and opinion of the *Klayman* holding.

Amicus Curiae Brief

On April 3, 2014, the Center for National Security Studies filed an *amicus curiae* brief explaining why it believes that 50 U.S.C. §1861 does not authorize the collection of bulk telephony metadata. The *amicus* brief made a number of thoughtful points, the merits of which I have analyzed. Notwithstanding the Center's arguments, I find the authority requested by the FBI through the instant Application meets the requirements of the statute, and that the collection of bulk telephony metadata may be authorized under the terms of the statute.

⁴ Following a declassification review by the Executive Branch, the Court published the March 20 Opinion and Order issued in Docket Number BR 14-01 in redacted form on April 25, 2014.

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

Declassified by the DNI June 27, 2014

~~TOP SECRET//SI//NOFORN~~*Conclusion*

The unauthorized disclosure of the bulk telephony metadata collection more than a year ago led to many written and oral expressions of opinions about the legality of collecting telephony metadata. Congress is well aware that this Court has interpreted the provisions of 50 U.S.C. § 1861 to permit this particular collection, and diverse views about the collection have been expressed by individual members of Congress. In recent months, Congress has contemplated a number of changes to the Foreign Intelligence Surveillance Act, a few of which would specifically prohibit this collection. Congress could enact statutory changes that would prohibit this collection going forward, but under the existing statutory framework, I find that the requested authority for the collection of bulk telephony metadata should be granted. Courts must follow the law as it stands until the Congress or the Supreme Court changes it.

In light of the public interest in this particular collection and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion, Judge McLaughlin's October 11 Memorandum, and Judge Collyer's March 20 Opinion and Order, I request pursuant to FISC Rule 62 that this Memorandum Opinion and Accompanying Primary Order also be published, and I

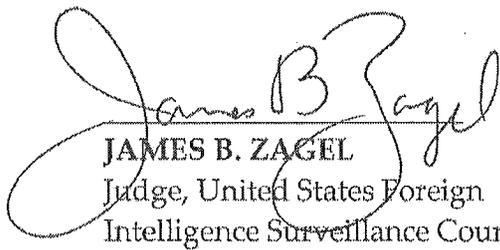
~~TOP SECRET//SI//NOFORN~~

Declassified by the DNI June 27, 2014

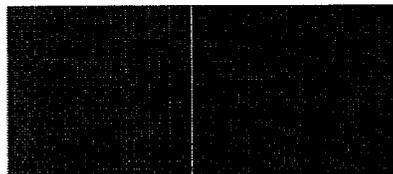
~~TOP SECRET//SI//NOFORN~~

direct such request to the Presiding Judge as required by the Rule.

ENTERED this 19th day of June, 2014.


JAMES B. ZIGEL
Judge, United States Foreign
Intelligence Surveillance Court

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



Declassified by the DNI June 27, 2014

~~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

14 - 9 6

PRIMARY ORDER

A verified application having been made by the Deputy 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

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

Derived from: Pleadings in the above-captioned docket
Declassify on: 20 June 2039

Declassified by the DNI June 27, 2014

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

amended, requiring the 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

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

¹ The Honorable Rosemary M. Collyer issued an Opinion and Order finding that, under *Smith v. Maryland*, 442 U.S. 735 (1979), this bulk production of non-content call detail records does not involve a search or seizure under the Fourth Amendment. See FISC docket no. BR 14-01, Opinion and Order issued on March 20, 2014 (under seal and pending consideration for unsealing, declassification, and release). This authorization relies on that analysis of the Fourth Amendment issue. In addition, the Court has carefully considered opinions issued by Judges Eagan and McLaughlin in docket numbers BR 13-109 and BR 13-158, respectively, as well as the decision in *Smith v. Obama*, No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014), *American Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013), *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013), *U.S. v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013), and the Brief of Amicus Curiae for Center for National Security Studies on the Lack of Statutory Authority for this Court's Bulk Telephony Metadata Orders, Misc. 14-01 (FISC filed Apr. 3, 2014), available at <http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Brief-1.pdf>.

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

Declassified by the DNI June 27, 2014

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

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 14-67 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, and as further explained in the accompanying Memorandum Opinion, 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 ██████████ 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"² created by ██████████.

² 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))

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

Declassified by the DNI June 27, 2014

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

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 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 or has received as a result of this Order or predecessor Orders of this Court requiring the production to NSA of

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~~

Declassified by the DNI June 27, 2014

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

telephony metadata pursuant to 50 U.S.C. § 1861, NSA shall strictly adhere to the minimization procedures set out at subparagraphs A. through G. below; provided, however, that the Government may take such actions as are permitted by the Opinion and Order of this Court issued on March 12, 2014, in docket number BR 14-01, subject to the conditions and requirements stated therein, including the requirement to notify this Court promptly of any material developments in civil litigation pertaining to such telephony metadata.

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.³ The BR metadata shall carry unique markings such 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

³ 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 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.

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

Declassified by the DNI June 27, 2014

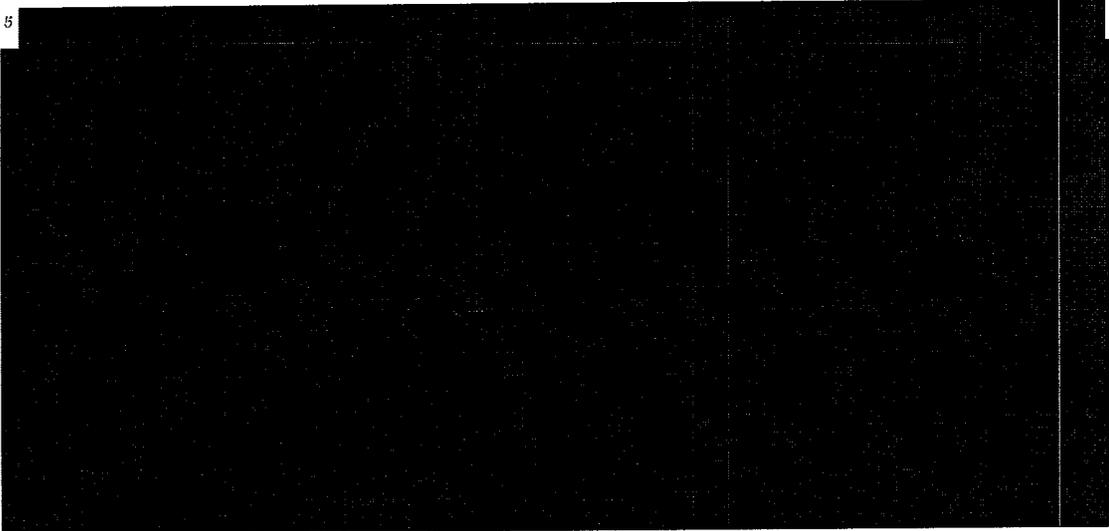
~~TOP SECRET//SI//NOFORN~~

authorized personnel who have received appropriate and adequate training.⁴

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 terms⁵ 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, 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

⁴ 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.



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

Declassified by the DNI June 27, 2014

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

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. The government may request, by motion and on a case-by-case basis, permission from the Court for NSA⁶ to use specific selection terms that satisfy the reasonable articulable suspicion (RAS) standard⁷ as "seeds" to query the BR metadata

⁶ 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.

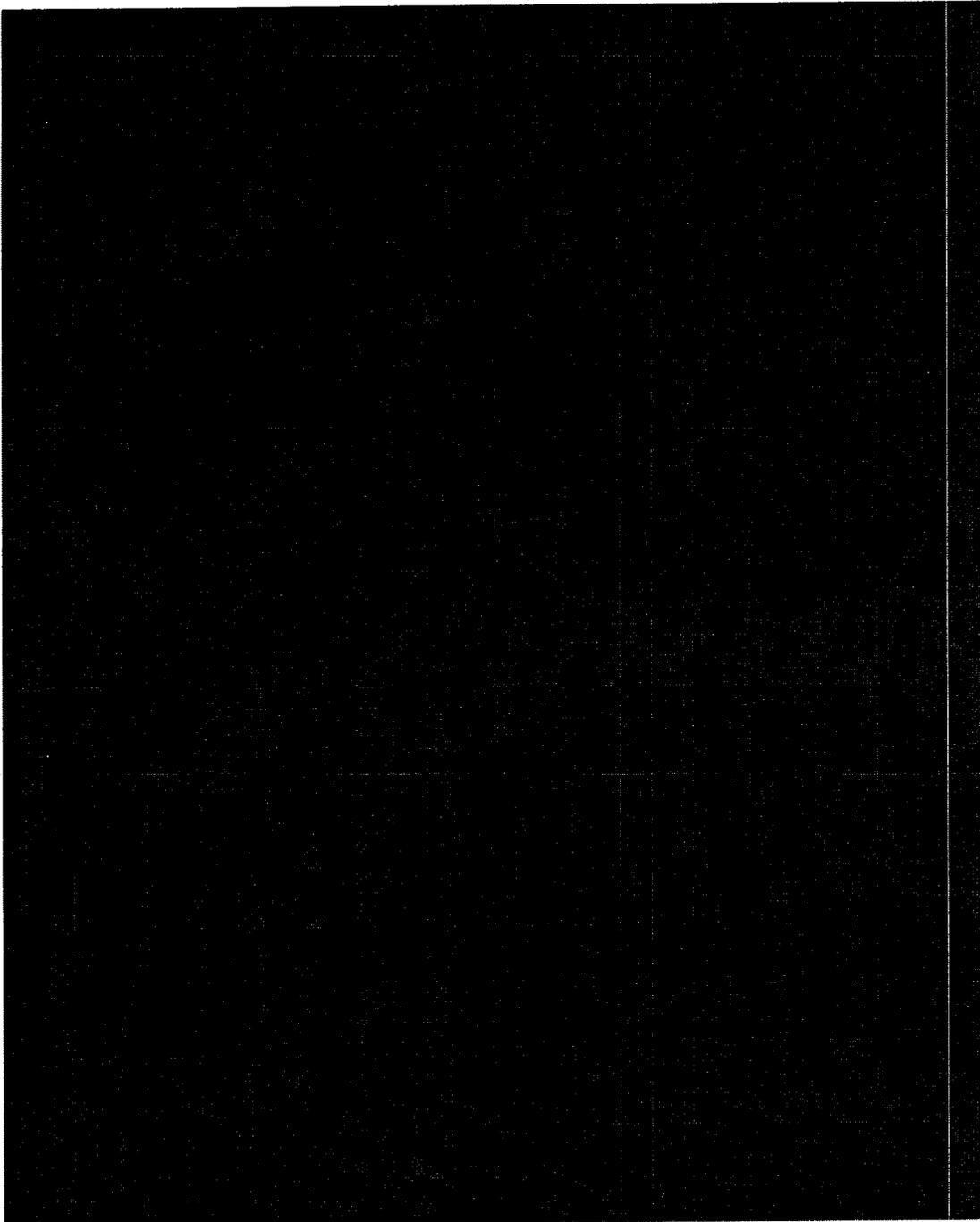
⁷ The reasonable articulable suspicion standard is met when, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED] provided, however, that any selection term reasonably believed to be used by a United States (U.S.) person shall not be regarded as associated with [REDACTED] solely on the basis of activities that are protected by the First Amendment to the Constitution. In the event the emergency provisions the Court's Primary Order are invoked by the Director or Acting Director, NSA's Office of General Counsel (OGC), in consultation with the Director or Acting Director will first confirm that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [REDACTED]

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

Declassified by the DNI June 27, 2014

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

 solely on the basis of activities that are protected by the First Amendment to the Constitution.



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

Declassified by the DNI June 27, 2014

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

to obtain contact chaining information, within two hops of an approved "seed", for purposes of obtaining foreign intelligence information. In addition, the Director or Acting Director of NSA may authorize the emergency querying of the BR metadata with a selection term for purposes of obtaining foreign intelligence information, within two hops of a "seed", if: (1) the Director or Acting Director of NSA reasonably determines that an emergency situation exists with respect to the conduct of such querying before an order authorizing such use of a selection term can with due diligence be obtained; and (2) the Director or Acting Director of NSA reasonably determines that the RAS standard has been met with respect to the selection term. In any case in which this emergency authority is exercised, the government shall make a motion in accordance with the Primary Order to the Court as soon as practicable, but



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

Declassified by the DNI June 27, 2014

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

not later than 7 days after the Director or Acting Director of NSA authorizes such query.⁸

(i) Any submission to the Court under this paragraph shall, at a minimum, specify the selection term for which query authorization is sought or was granted, provide the factual basis for the NSA's belief that the reasonable articulable suspicion standard has been met with regard to that selection term and, if such query has already taken place, a statement of the emergency necessitating such query.⁹

(ii) NSA shall ensure, through 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.¹⁰ Whenever

⁸ In the event the Court denies such motion, the government shall take appropriate remedial steps, including any steps the Court may direct.

⁹ For any selection term that is subject to ongoing Court-authorized electronic surveillance, pursuant to 50 U.S.C. § 1805, based on this Court's finding of probable cause to believe that the selection term is being used or is about to be used by agents of [REDACTED]

[REDACTED] including those used by U.S. persons, the government may use such selection terms as "seeds" during any period of ongoing Court-authorized electronic surveillance without first seeking authorization from this Court as described herein. Except in the case of an emergency, NSA shall first notify the Department of Justice, National Security Division of its proposed use as a seed any selection term subject to ongoing Court-authorized electronic surveillance.

¹⁰ NSA has implemented technical controls, which preclude any query for intelligence analysis purposes with a non-RAS-approved seed.

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

Declassified by the DNI June 27, 2014

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

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.¹¹

(iii) The Court's finding that a selection term is associated with [REDACTED]

[REDACTED]

[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.^{12,13}

(iv) Queries of the BR metadata using RAS-approved selection terms for purposes of obtaining foreign intelligence information may occur by manual analyst

¹¹ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

¹² The Court understands that from time to time the information available to NSA 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, the government's submission shall specify the time frame for which the selection term is or was associated with [REDACTED]

[REDACTED] In the event that the RAS standard is met, analysts conducting manual queries using that selection term shall properly minimize information that may be returned within query results that fall outside of that timeframe.

¹³ 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]

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

Declassified by the DNI June 27, 2014

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

query only. Queries of the BR metadata to obtain foreign intelligence information shall return only that metadata within two "hops" of an approved seed.¹⁴

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 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)

¹⁴ The first "hop" from a seed returns results including all identifiers (and their associated metadata) with a contact and/or connection with the seed. The second "hop" returns results that include all identifiers (and their associated metadata) with a contact and/or connection with an identifier revealed by the first "hop."

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.

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

Declassified by the DNI June 27, 2014

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

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 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. Notwithstanding the above requirements, NSA may share the results from intelligence analysis queries of the BR metadata, including United States person information, with Legislative Branch personnel to facilitate 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.

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~~

Declassified by the DNI June 27, 2014

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

(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 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

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~~

Declassified by the DNI June 27, 2014

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

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.

(vi) Prior to implementation of any automated query processes, such 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 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, other than

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

Declassified by the DNI June 27, 2014

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

Executive Branch or Legislative Branch personnel receiving such results for their purposes that are exempted from the dissemination requirements of paragraph (3)D above. 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 counterterrorism information or to assess its importance. 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.

- Remainder of this page intentionally left blank -

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

Declassified by the DNI June 27, 2014

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

This authorization regarding [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] expires on the 12th day

of September, 2014, at 5:00 p.m., Eastern Time.

Signed 19 June 2014 16:35 Eastern Time
Date Time


JAMES B. ZAGEL
Judge, United States Foreign
Intelligence Surveillance Court

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

[REDACTED]

~~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

Under Seal

Docket No. BR 14-01

OPINION AND ORDER

On January 22, 2014, [REDACTED]

[REDACTED] filed a
Petition pursuant to 50 U.S.C. § 1861(f)(2)(A) and Rule 33 of the Foreign Intelligence
Surveillance Court ("FISC" or "the Court") Rules of Procedure "to vacate, modify, or
reaffirm" a production order issued [REDACTED] January 3, 2014 ("Petition"). After
conducting the initial review required by Section 1861(f)(2)(A)(ii) and FISC Rule 39, the
Court determined that the Petition is not frivolous and issued a Scheduling Order
pursuant to FISC Rule 39(c) on January 23, 2014. Pursuant to the Scheduling Order, the
United States filed its Response to the Petition on February 12, 2014 ("Response"). The
Petition is now ripe for review. For the reasons set forth below, the Court concludes

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

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

that the Petition provides no basis for vacating or modifying the production order. Accordingly, that order is affirmed and remains in full force and effect until it expires by its own terms on March 28, 2014.

I. BACKGROUND

On January 3, 2014, this Court issued a Primary Order approving the Government's application pursuant to Section 501 of the Foreign Intelligence Surveillance Act of 1978, codified at 50 U.S.C. § 1861, as amended ("FISA"), for orders requiring the production to the National Security Agency ("NSA"), in bulk and on an ongoing basis, of non-content call detail records or "telephony metadata" created by certain telecommunications carriers [REDACTED] ("January 3 Primary Order"). Jan. 3 Primary Order at 3.¹ [REDACTED] served with one of the resulting production orders on the same date and has complied with the order, as it has with previous orders requiring the bulk production of telephony metadata. See Pet. at 2; id. Exh. 1 (copy of Jan. 3, 2014 "Secondary Order" issued [REDACTED]). The Primary Order and Secondary Order expire on March 28, 2014, at 5:00 p.m. Eastern Time. See Jan. 3 Primary Order at 18; Pet. Exh. 1 (Secondary Order) at 4.

FISA permits the recipient of a production order issued under Section 1861 to

¹ The January 3 Primary Order is available in redacted form at <http://www.uscourts.gov/uscourts/courts/fisc/br14-01-primary-order.pdf>.

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

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

"challenge the legality of that order by filing a petition" with this Court. 50 U.S.C. § 1861(f)(2)(A)(i); see also FISC Rule 33(a).² It further provides that "[a] judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful." 50 U.S.C. § 1861(f)(2)(B). If the judge does not modify or set aside the production order, the judge must "immediately affirm such order, and order the recipient to comply therewith." Id.; see also FISC Rule 41(b). The judge must also provide a "written statement . . . of the reasons" for modifying, setting aside, or affirming the production order. 50 U.S.C. § 1861(f)(2)(a)(iii); FISC Rule 41(a).

In its Petition [REDACTED] Klayman v.

Obama, Civil Action No. 13-0851 (RJL) (D.D.C. June 6, 2013), a suit in which the plaintiffs assert, among other things, that a production order issued to Verizon by this Court in Docket No. BR 13-80, [REDACTED] is

² Such a petition must be filed "under seal." 50 U.S.C. § 1861(f)(5). After it is filed, the petition must "immediately" be assigned to one of the three FISC judges who reside within 20 miles of the District of Columbia. 50 U.S.C. § 1861(f)(2)(A)(ii); see also FISC Rule 38(a). Within 72 hours, the assigned judge must conduct an initial review of the petition. 50 U.S.C. § 1861(f)(2)(A)(iii); see also FISC Rule 39(a). If the assigned judge concludes that the petition is frivolous, he or she must "immediately deny the petition and affirm the production order." 50 U.S.C. § 1861(f)(2)(A)(ii); see also FISC Rule 39(b). If the assigned judge determines that the petition is not frivolous, the judge must "promptly consider the petition." 50 U.S.C. § 1861(f)(2)(A)(ii); see also FISC Rule 39(c).

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

Page 3

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

unconstitutional. See Pet. at 2. On December 16, 2013, Judge Richard J. Leon issued a Memorandum Opinion in Klayman, a copy of which is attached as Exhibit 2 to the Petition, holding that the plaintiffs are likely to succeed on their claim that the bulk collection of call detail records authorized by the production order issued to Verizon in FISC Docket No. BR 13-80 is "an unreasonable search under the Fourth Amendment." See id. (citing Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013)). Judge Leon ordered that the Government cease collection of "any telephony metadata associated with [the plaintiffs'] personal Verizon accounts" and destroy any such metadata in its possession, but he stayed the order pending appeal. See id. (citing Klayman, 957 F. Supp. 2d at 43).

[REDACTED] the Petition "arises entirely from [REDACTED] Judge Leon's Memorandum [Opinion]," and, specifically, his conclusion that Supreme Court's decision in Smith v. Maryland, 442 U.S. 735 (1979), is "inapplicable to the specific activities mandated by the [Section] 1861 order at issue in the Klayman litigation." Id. at 3-4. [REDACTED] in its Petition that this Court may have "considered and rejected" Judge Leon's analysis in issuing the January 3, 2014 production order, but that the Secondary Order [REDACTED] does not refer to Judge Leon's decision and that [REDACTED] not been provided with the Court's

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

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

underlying legal analysis." *Id.* at 4. [REDACTED] asks this Court to "vacate, modify, or reaffirm the current production order in light of the Memorandum Opinion issued in Klayman." *Id.*³ [REDACTED] it is complying with the production order and "will continue to comply fully with that order unless otherwise directed by the Court." *Id.*

The Government asserts in its Response that

[t]he Primary Order in the above-captioned docket number makes clear that the Court, in entertaining and ultimately ruling upon the Government's application, carefully considered not only the opinions entered by Judges Eagan and McLaughlin of this Court in docket numbers BR 13-109 and BR 13-158, respectively,^[1] and the decision issued by the United States District Court for the Southern District of New York in American Civil Liberties Union v. Clapper, [959] F. Supp. 2d [724] . . . (Dec. 27, 2013), but also [Judge Leon's Memorandum Opinion in Klayman].

³ Prior to the filing of [REDACTED] "no holder of records who ha[d] received an Order to produce bulk telephony metadata" or any other tangible things pursuant to Section 1861 "ha[d] challenged the legality of such an Order." In Re Application of the FBI for an Order Requiring the Production of Tangible Things, Docket No. BR 13-109, 2013 WL 5741573, at *5 (FISA Ct. Aug. 29, 2013) (hereinafter "Aug. 29, 2013 Amended Op.").

⁴ See Aug. 29, 2013 Amended Op., 2013 WL 5741573 (Eagan, J.); In Re Application of the FBI for an Order Requiring the Production of Tangible Things, Docket No. BR 13-158, Memorandum (FISA Ct. Oct. 11, 2013) (McLaughlin, J.), available at <http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf> (hereinafter "Oct. 11, 2013 Mem.").

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

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

Response at 3 (citing Jan. 3 Primary Order at 2 n.1).⁵ In light of that statement, the Government asserts that "it is appropriate for the Court to affirm its January 3, 2014 Secondary Order [REDACTED] and to order [REDACTED] compliance with that production order." *Id.*

II. ANALYSIS

[REDACTED] not contest that the production order at issue here is consistent with the requirements of Section 1861. *See* Petition at 2-4. The only question raised in the Petition is whether the production order is unlawful under the Fourth Amendment in light of Judge Leon's December 16 opinion in *Klayman*. *See id.*, at 4. It is true, as the Government observes in its Response, that the Court stated in the January 3 Primary Order that it had carefully considered Judge Leon's opinion in *Klayman* before issuing the requested production orders. *See* Jan. 3 Primary Order at 2 n.1. Nevertheless,

[REDACTED] has filed a Petition under Section 1861(f), the undersigned Judge must consider the issue anew.

A. Standing.

Before turning to the Fourth Amendment issue raised [REDACTED] the Court must first address the question of standing. In challenging the production order,

⁵ The Government apparently did not share the Primary Order with [REDACTED] until [REDACTED] had filed its Petition. *See* Pet. at 4.

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

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

 not its own Fourth Amendment rights, but those of its customers. See Pet. at 3-4. Litigants ordinarily cannot assert the rights of third parties in an Article III court. See In Re Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1008 (FISA Ct. Rev. 2008) (citing Hinck v. United States, 550 U.S. 501, 510 n.3 (2007), and Warth v. Seldin, 422 U.S. 490, 499 (1975)). But, as the Foreign Intelligence Surveillance Court of Review explained in addressing a similar challenge brought under a similar but now expired provision of FISA, “that prudential limitation may in particular cases be relaxed by congressional action.” Id. (citing Warth, 422 U.S. at 501).⁶ “Thus, if Congress, either expressly or by fair implication, cedes to a party the right to bring suit based on the legal rights or interests of others, that party has standing to sue; provided, however, that constitutional standing requirements are satisfied.” Id. (citing Warth, 422 U.S. at 500-01).

To have standing under Article III of the Constitution, “the suitor must plausibly

⁶ In In Re Directives, the Court of Review concluded that a service provider that had received a “directive” pursuant to the Protect America Act (“PAA”) – a now-expired provision of FISA that was codified at 50 U.S.C. § 1805a-c – had standing to assert the Fourth Amendment rights of its customers in a petition filed with the FISC. 551 F.3d at 1008-09. The PAA authorized the Executive Branch to direct communications service providers to assist it in acquisitions targeting persons located outside the United States. Id. at 1006. It also provided that the recipient of a directive “may challenge the legality of that directive” in a petition to the FISC. Id. (quoting now-expired 50 U.S.C. § 1805b(h)(1)(A)).

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

Page 7

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

allege that it has suffered an injury, which was caused by the defendant, and the effects of which can be addressed by the suit." *Id.* (citing *Warth*, 422 U.S. at 498-99). The Court is satisfied [REDACTED] has Article III standing here. Like [REDACTED] [REDACTED] "faces an injury in the nature of the burden that it must shoulder" to provide the Government with call detail records. *Id.* That injury is "obviously and indisputably caused by the [G]overnment" through the challenged Secondary Order, and this Court is capable of redressing the injury by vacating or modifying the order. See id.

The Court is also satisfied that Congress has [REDACTED] as the recipient of a Section 1861 production order, the right to bring a challenge in this Court to enforce the rights of its customers. As noted above, FISA states that the recipient of a Section 1861 production order "may challenge the legality of that order by filing a petition" with the FISC. 50 U.S.C. § 1861(f)(2)(A)(i). As with the similar provision at issue in *In Re Directives*, Section 1861(f) "does nothing to circumscribe the types of claims of illegality that can be brought." *In Re Directives*, 551 F.3d at 1009 (discussing now-expired 50 U.S.C. § 1805b(h)(1)(A)), the PAA provision described above in note 6). Indeed, it provides that this Court may modify or set aside a production order "if the judge finds that such order does not meet the requirements of this section or is

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

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

otherwise unlawful” thus suggesting that Congress intended to permit the recipients of production orders to bring a range of challenges. 50 U.S.C. § 1861(f)(2)(B) (emphasis added). The Court therefore concludes that Section 1861(f) “grants an aggrieved service provider a right of action and extends that right to encompass claims brought by it on the basis of [its] customers’ rights.” In Re Directives, 551 F.3d at 1009 (reaching the same conclusion regarding the similar language of the PAA).

B. The Fourth Amendment.

Turning now to the merits of the Fourth Amendment issue, this Court finds Judge Leon’s analysis in Klayman to be unpersuasive and concludes that it provides no basis for vacating or modifying the Secondary Order issued [REDACTED] January 3,

2014. The Fourth Amendment provides that:

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 person or thing to be seized.

U.S. Const., Amend. IV. For purposes of the Fourth Amendment, a “search” occurs when the Government violates a person’s reasonable expectation of privacy, see Smith, 442 U.S. at 740 (citing cases), or when the Government physically intrudes on a protected area for the purpose of acquiring information, United States v. Jones, 132 S.

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

Page 9

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

Ct. 945, 951 (2012).

1. Smith v. Maryland and its Progeny.

In Smith, investigators acting without a warrant caused the telephone company to install a pen register at its offices to record the numbers dialed on the home phone of Smith, who was suspected of robbing and then harassing a woman through anonymous phone calls. Smith, 442 U.S. at 737. The pen register confirmed that the calls had originated from Smith's phone. Id. The dialing information was used to obtain a warrant to search Smith's home, and he was later convicted. Id. at 737-38. The Supreme Court rejected Smith's claim that the use of the pen register violated the Fourth Amendment, holding that it was not a search. Id. at 745-46. The Court explained that:

[w]hen he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed.

Id. at 744. The Court observed that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44 (citing other cases applying the same third-party disclosure principle). Other courts have relied on Smith in concluding that the Fourth

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

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

Amendment does not apply to “trap and trace” devices, which function like pen registers but record the originating numbers of incoming calls, or to information such as the date, time, and duration of calls. *See, e.g., United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009); *United States Telecom Ass’n v. FCC*, 227 F.3d 450, 454, 459 (D.C. Cir. 2000); *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990).

The information [REDACTED] produces to NSA as part of the telephony metadata program is indistinguishable in nature from the information at issue in *Smith* and its progeny. It includes dialed and incoming telephone numbers and other numbers pertaining to the placing or routing of calls, as well as the date, time, and duration of calls. *See* Pet. Exh. 1 (Secondary Order) at 2.⁷ It does not include the “contents” of any communications as defined in 18 U.S.C. § 2510; the name, address, or financial information of any subscriber or customer; or cell site location information. *See id.* Accordingly, two judges of this Court (in addition to the judge who issued the January 3 Primary Order in this docket) and two federal district courts have recently concluded

⁷ The Secondary Order states that “[t]elephony 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.” Pet. Exh. 1 (Secondary Order) at 2 (*italics in original*).

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

Page 11

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

that Smith is controlling with respect to the bulk telephony metadata produced to NSA. See Clapper, 959 F. Supp. 2d at 749-52 (Pauley, J.); United States v. Moalin, Case No. 10cr4246 JM, 2013 WL 6079518, at *7-*8 (S.D. Cal. Nov. 18, 2013) (Miller, J.); Oct. 11, 2013 Mem. at 4-5 (McLaughlin, J.); Aug. 29, 2013 Amended Op., 2013 WL 5741573, at *2-*3 (Eagan, J.).

2. *Judge Leon's Analysis in Klayman.*

Judge Leon acknowledged in Klayman that "what metadata *is* has not changed over time. As in Smith, the *types* of information at issue [here] are relatively limited: phone numbers dialed, date, time, and the like." 957 F. Supp. 2d at 35 (italics in original). He nevertheless declined to follow Smith, providing four reasons why, in his view, the NSA telephony metadata program "is so different from a simple pen register that Smith is of little value in assessing whether [it] constitutes a Fourth Amendment search." Id. at 32. First, Judge Leon asserted that the pen register in Smith lasted only thirteen days, with no indication from the Supreme Court "that it expected the Government to retain those limited phone records once the case was over." Id. The NSA program, on the other hand, "involves the creation and maintenance of a historical database containing *five years'* worth of data," and might "go on for as long as America is combating terrorism, which realistically could be forever!" Id. (italics and

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

Page 12

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

exclamation point in original).

Second, Judge Leon asserted, "the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and the telecom companies." *Id.* (italics in original). The pen register in *Smith* involved the phone company's response to a "one time, targeted request for data regarding an individual," whereas the NSA program involves the daily production of metadata, in bulk. *Id.* at 33. While people might expect phone companies to "occasionally provide information to law enforcement," Judge Leon expressed doubt that "citizens expect all phone companies to conduct what is effectively a joint intelligence-gathering operation with the Government." *Id.*

Third, Judge Leon asserted, "the almost-Orwellian technology" that enables the Government to store and analyze phone metadata following its acquisition is "unlike anything that could have been conceived in 1979." *Id.* According to Judge Leon, the Government uses the "most advanced twenty-first century tools, allowing it to 'store such records and efficiently mine them for information years into the future,'" and to do so cheaply and surreptitiously, thus evading the "ordinary checks that constrain abusive law enforcement practices: limited police . . . resources and community

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

Page 13

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

hostility.” Id. (quoting Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring)).

Fourth, and “*most importantly*,” according to Judge Leon, “the nature and quantity of the information contained in people’s telephony metadata [today] is much greater” than it was at the time of Smith. Id. at 34 (*italics in original*). Because more people use phones (and, in particular, cellular telephones) and use them more frequently now than in 1979, Judge Leon asserted that the “the metadata from each person’s phone ‘reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,’” that “could not have been gleaned from a data collection in 1979.” Id. at 36 (quoting Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring)). “Records that once would have revealed a few scattered files of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person’s life.” Id. (citing United States v. Maynard, 615 F.3d 544, 562-63 (D.C. Cir. 2010), aff’d sub nom United States v. Jones, 132 S. Ct. 945 (2012)).

3. *Smith Remains Controlling Notwithstanding Klayman.*

This Court respectfully disagrees with Judge Leon’s reasons for deviating from Smith. To begin with, Judge Leon focused largely on what happens (and what could happen) to the telephony metadata after it has been acquired by NSA – e.g., how long the metadata could be retained and how the Government could analyze it using

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

Page 14

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

sophisticated technology. Smith and the Supreme Court's other decisions applying the third-party disclosure principle make clear that this focus is misplaced in assessing whether the production of telephony metadata constitutes a search under the Fourth Amendment.

Smith reaffirmed that the third-party disclosure principle – i.e., the rule that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” Smith, 442 U.S. at 743-44 (citing cases) – applies regardless of the disclosing person's assumptions or expectations with respect to what will be done with the information following its disclosure. The Supreme Court emphasized:

“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.”

Smith, 442 U.S. at 744 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)) (emphasis added). Because the disclosing person assumes the risk of further disclosure by the third party, the Court explained it is “unreasonable” for him “to expect his . . . records to remain private.” Id. The Supreme Court's other third-party disclosure cases are also clear and consistent on this point. See Miller, 425 U.S. at 443 (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966);

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

Page 15

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

Lopez v. United States, 373 U.S. 427 (1963)); 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.") (emphasis added).⁸

Applying this rationale, the Supreme Court rejected Smith's contention that he had a legitimate expectation of privacy in the dialing information for the incriminating phone calls because they were local calls for which the phone company would not have recorded such information in the ordinary course of business:

The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had the facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be

⁸ Bond v. United States, 529 U.S. 334 (2000), cited by Judge Leon, see 957 F. Supp. 2d at 33 n.47, did not involve the disclosure of information to a third party and does not support a different approach here. In Bond, the Supreme Court held that a law enforcement agent conducted a search of a bus passenger's carry-on bag by squeezing it in an effort to determine what was inside. Id. at 338-39. The Court explained that while a bus passenger might expect others to touch or move a carry-on bag he places in the overhead compartment, he does not reasonably expect that others "will feel the bag in an exploratory manner." Id. Unlike the passenger in Bond, who "sought to preserve privacy by using an opaque bag and placing that bag directly above his seat," id. at 338, a telephone user who is making a call fully divulges to the phone company the numbers he dials.

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

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

divulged to police.

Smith, 442 U.S. at 745.

If a person who voluntarily discloses information can have no reasonable expectation concerning limits on how the recipient will use or handle the information, it necessarily follows that he or she also can harbor no such expectation with respect to how the Government will use or handle the information after it has been divulged by the recipient. Smith itself makes clear that once a person has voluntarily conveyed dialing information to the telephone company, he forfeits his right to privacy in the information, regardless of how it might be later used by the recipient or the Government. See id. Accordingly, Judge Leon's concerns regarding NSA's retention and analysis of the call detail records are irrelevant in determining whether a Fourth Amendment search has occurred.

For the same reason, Judge Leon's assertions regarding citizens' expectations with respect to the "relationship . . . between the Government and the telecom companies," see Klayman, 957 F. Supp. 2d at 32-33, also provide no basis for departing from Smith. Under Smith, Miller, and the other third-party disclosure cases cited above, any such expectations or assumptions on the part of telephone users who have disclosed their dialing information to the phone company have no bearing on the

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

Page 17

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

question whether a search has occurred. See Smith, 442 U.S. at 744.⁹

Judge Leon's assertions regarding the nature and quantity of telephony metadata acquired by NSA likewise fail to justify deviating from the clear holding of Smith. Judge Leon acknowledged that the types of information acquired by NSA in the telephony metadata program are "limited" to "phone numbers dialed, date, time, and the like." 957 F. Supp. 2d at 35. He nevertheless stressed that phones today, and, in particular, cell phones, are not just telephones, but "multi-purpose devices" that can be used to access Internet content, and as maps, music players, cameras, text messaging

⁹ The two decisions cited by Judge Leon on this point are not to the contrary. See Klayman, 957 F. Supp. 2d at 33. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989), is not a Fourth Amendment case at all. And Ferguson v. City of Charleston, 532 U.S. 67 (2001), is distinguishable. There, the Court addressed a program involving the nonconsensual urine testing of pregnant women for illegal drugs by a state hospital, which shared positive results with police. See id. at 70-73. The Court examined the relationship between the hospital and the police not in determining whether the urine tests constituted searches within the meaning of the Fourth Amendment (the Court stated that they "indisputably" did, id. at 76), but in assessing whether the purpose of the program was law enforcement or something different. See id. at 82-85. At issue here is whether the NSA telephony metadata program involves a search in the first place.

Furthermore, Judge Leon's suggestion that the NSA telephony metadata program, like the drug testing program in Ferguson, entails "the service provider[s] collect[ion of] information for law enforcement purposes," Klayman, 957 F. Supp. 2d. at 33, is incorrect. As he acknowledges earlier in his opinion, the information produced to NSA consists of "telephony metadata records . . . which the companies create as part of their business of providing telecommunications services to customers." Id. at 15 (emphasis added).

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

Page 18

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

devices, and even as “lighters for people to hold up at rock concerts.” *Id.* at 34. Judge Leon asserted that people today therefore have an “entirely different relationship” with their telephones than they did when *Smith* was decided. *Id.* at 36. But none of these additional functions generates any information that is being collected by NSA as part of the telephony metadata program, which as discussed above, involves only non-content records concerning the placing and routing of telephone calls. Accordingly, such changes are irrelevant here.¹⁰

Judge Leon also repeatedly emphasized the total quantity of telephony metadata obtained and retained by NSA.¹¹ That focus is likewise misplaced under settled

¹⁰ Judge Leon also noted that “telephony metadata” for cell phones also “can reveal the user’s location” but stated that “[his] decision . . . does *not* turn on whether the NSA has in fact collected that data as part of the bulk telephony metadata program” *Id.* at 36 n.57 (italics in original). The metadata produced in this matter does not include cell site location information or Global Positioning System (“GPS”) data. *See* Jan. 3 Primary Order at 4; Pet. Exh. 1 (Secondary Order) at 2.

¹¹ *See Klayman*, 957 F. Supp 2d. at 30 (articulating question presented as “whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their metadata along with the metadata of hundreds of millions of other citizens” without particularized suspicion) (emphasis added); *id.* at 33 (“The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction.”) (emphasis added); *id.* at 33 n.48 (“The unprecedented scope and technological sophistication of the NSA’s program distinguish it not only from the *Smith* pen register, but also from metadata collections performed as part of routine criminal

(continued...)

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

Page 19

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

Supreme Court precedent. The Court has repeatedly reaffirmed that Fourth Amendment rights are "personal rights" that "may not be vicariously asserted." See Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (citing cases; citations and internal quotation marks omitted); accord Minnesota v. Carter, 525 U.S. 83, 88 (1998). Accordingly, the aggregate scope of the collection and the overall size of NSA's database are immaterial in assessing whether there any person's reasonable expectation of privacy has been violated such that a search under the Fourth Amendment has occurred. To the extent that the quantity of the metadata collected by NSA is relevant, it is relevant only on a user-by-user basis. The pertinent question is whether a particular user has a reasonable expectation of privacy in the telephony metadata associated with his or her own calls. For purposes of determining whether a search under the Fourth Amendment has occurred, it is irrelevant that other users' information is also being collected and that the aggregate amount acquired is very large. Cf. United States v. Dionisio, 410 U.S. 1, 13 (1973) (grand jury subpoena not "rendered unreasonable by the fact that many others were subjected to the same compulsion").

Properly viewed on a user-by-user basis, the NSA telephony metadata program

¹¹(...continued)
investigations.") (emphasis added); id. at 34 (citing statistics regarding the number of phones and cell phones in use today, as compared to 1979).

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

Page 20

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

is consistent with Supreme Court precedent, which time and technology have not affected. United States v. Miller, the principal precedent relied upon by the Court in Smith, was, notably, a case involving the compelled production of records of customer activities. The Court held that a bank customer had no legitimate expectation of privacy in three-and-a-half months worth of bank records acquired from two banks. Miller, 425 U.S. at 443. The records in question consisted of checks, deposit slips, monthly statements, and financial statements and were turned over to police investigators pursuant to a grand jury subpoena. Id. at 438. Invoking the same principle that would later be relied upon in Smith, the Court explained that the documents in question “contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” Id. at 442. The Court further stated that “[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.” Id. at 433.

It is far from clear to this Court that even years’ worth of non-content call detail records would reveal more of the details about a telephone user’s personal life than several months’ worth of the same person’s bank records. Indeed, bank records are likely to provide the Government directly with detailed information about a customer’s personal life – e.g., the names of the persons with whom the customer has had financial

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

Page 21

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

dealings, the sources of his income, the amounts of money he has spent and on what forms of goods and services, the charities and political organizations that he supports – that call detail records simply do not, by themselves, provide. Miller, which was decided in 1976, substantially undermines Judge Leon’s conclusion that Smith does not apply to the NSA telephony metadata program because the metadata from each person’s phone reveals so much about a person “that could not have been gleaned from a data collection in 1979,” when Smith was decided. See Klayman, 957 F. Supp. 2d at 36. Many more personal details could immediately and directly be obtained from bank records such as those in the production approved by the Court in Miller without raising Fourth Amendment concerns.

Moreover, it must be emphasized that the non-content telephony metadata at issue here is particularly limited in nature and subject to strict protections that do not apply to run-of-the-mill productions of similar information in criminal investigations. The call detail records acquired by NSA do not include subscriber names or addresses or other identifying information. See Pet. Exh. 1 (Secondary Order) at 2. Rather, such information can be determined by the Government for any particular piece of metadata only by resorting to other investigative resources or tools, such as grand jury subpoenas or national security letters. Furthermore, pursuant to this Court’s Primary Order, the

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

Page 22

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

metadata can only be accessed for analytical purposes after NSA has established a reasonable articulable suspicion ("RAS") that the number to be used to query the data – the "seed" – is associated with one of the terrorist groups listed in the Order. See Jan. 3 Primary Order at 6-9 & nn. 8-9. Each query is limited to metadata within two (formerly three) "hops" of the seed. See id. at 11-12; Feb. 5, 2014 Order Granting Government's Motion to Amend the Court's Primary Order Dated January 3, 2014 ("Feb. 5 Order"), at 3-4, 9.¹² These protections further undercut Judge Leon's reliance on the perceived intrusiveness of the telephony metadata program as a basis for deviating from Smith.¹³

¹² The February 5 Order is available at <http://www.uscourts.gov/uscourts/courts/fisc/br-14-01-order.pdf>.

¹³ As originally issued by the Court, the January 3 Primary Order – like predecessor orders – required certain designated NSA officials to make the requisite RAS determinations. See Jan. 3 Primary Order at 7. Also like predecessor orders, the January 3 Primary Order permitted the query results to include the metadata for numbers within three "hops" of the querying seed. See id. at 10-11. The Court recently granted the Government's motion to amend the January 3 Primary Order to preclude NSA, except in the case of an emergency, from querying the repository of telephony metadata without first having obtained a determination by this Court that the RAS standard is satisfied for each querying seed. See Feb. 5 Order at 3-4, 9. The Court also granted the Government's request to limit query results to metadata for numbers within two "hops" of the querying seed. See id.

Whether the RAS determination requirement is applied with or without direct judicial involvement, it sharply restricts the Government's access to and use of the collected telephony metadata. The same is true of the restriction on the scope of query results, whether the limit is two or three "hops." Indeed, because these restrictions limit
(continued...)

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

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

4. United States v. Jones Does Not Support a Different Conclusion.

The Supreme Court's more recent decision in Jones provides no basis for departing from Smith with respect to the Government's acquisition of non-content telephony metadata. In Jones, law enforcement officers acting without a valid warrant surreptitiously attached a GPS device to the defendant's Jeep and used it to track his location for 28 days. Jones, 132 S. Ct. at 948. The district court denied Jones' motion to suppress in large part, holding that the GPS evidence acquired while the vehicle was on public roads was admissible under United States v. Knotts, 460 U.S. 276, 281 (1983) (use of radio beeper to track defendant's car on public roads did not violate any reasonable expectation of privacy). See id.

Following Jones' conviction, the court of appeals reversed on this point, holding that the use of the GPS device over 28 days was a search under the Fourth Amendment. Maynard, 615 F.3d at 558. In doing so, the court of appeals concluded that Knotts was not controlling and adopted a novel mode of analysis. See id., at 556-66. Rather than assessing the likelihood that Jones' discrete movements over the 28 days had

¹³(...continued)

NSA to looking for information on specific terrorist groups and not other persons, the vast majority of the metadata acquired by NSA is never reviewed by any person. See In Re Application of the FBI for an Order Requiring the Production of Tangible Things, 2013 WL 5741573, at *8 n.23.

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

Page 24

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

individually been exposed to the public, the court of appeals — applying a “mosaic” analysis similar to the one later used by Judge Leon in Klayman — considered whether his movements, viewed in the aggregate, were so exposed. See id. at 562. Because it was extremely unlikely that any single member of the public would actually observe the collective whole of Jones’ movements over the course of the GPS tracking, the court of appeals concluded that Jones had a reasonable expectation of privacy that had been violated by the tracking. See id. at 560 (“[T]he whole of a person’s movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil.”). The court of appeals denied the Government’s petition for rehearing en banc, with four judges dissenting. See United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010).

The Supreme Court affirmed the court of appeals, but on different grounds. The Court held in Justice Scalia’s majority opinion that the officers’ conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant’s vehicle, a constitutionally-protected area. Jones, 132 S. Ct. at 949, 953. The Court declined to address the question whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy, and therefore did not pass on the court of appeals’ novel

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

Page 25

A62

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

“mosaic” analysis of that question. Id. at 953-54. The Court cited Smith, but only in passing. See id. at 950. The Court’s opinion does not support Judge Leon’s conclusion that a modern telephone user has a legitimate expectation of privacy in the metadata relating to his calls, which is disclosed to the telephone company for the purpose of completing calls, or that the larger number of calls made in today’s world undermines Smith’s holding.

Judge Leon relied instead on the two concurring opinions in Jones. To be sure, those opinions express the view that the precise, pervasive monitoring by the Government of a person’s location might trigger Fourth Amendment protection even without any physical intrusion. See Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring); id. at 962-64 (Alito, J., concurring in the judgment). They also signal that five Justices of the Court may be ready to endorse a new mode of analysis similar to the “mosaic” theory adopted by the court of appeals in Maynard. See id. But the concurring opinions in Jones nevertheless fail to support deviation from Smith in connection with the NSA telephony metadata program.

Of course, the majority opinion in Jones is controlling, and, as discussed above, that opinion does not even reach the reasonable-expectation-of-privacy issue. Moreover, although the two concurring opinions address privacy, they suggest distinct

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

Page 26

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

analytical approaches and thus can hardly be read as having adopted a single, coherent principle or methodology for lower courts to apply. Justice Sotomayor's approach – on which Judge Leon appears to have modeled much of his analysis in Klayman, 957 F. Supp. 2d at 36 – looked to “whether police conduct collected so much information that it enabled police to learn about a person's private affairs ‘more or less at will.’” Orin S. Kerr, “The Mosaic Theory of the Fourth Amendment,” 111 Mich. L. Rev. 311, 328 (Dec. 2012) (quoting Jones, 132 S. Ct. at 955-56 (Sotomayor, J., concurring)). Justice Alito's opinion, in which three other Justices joined, focused instead on “whether the investigation exceeded society's expectations for how the police would investigate a particular crime.” Id. (citing 132 S. Ct. at 964 (Alito, J., concurring in the judgment)).¹⁴ These distinct approaches to the expectation-of-privacy question undercut Judge Leon's suggestion that the five concurring Justices in Jones can be viewed as a de facto majority on the issue. See Klayman, 957 F. Supp. 2d at 31 (stating that “five justices found that law enforcement's use of a GPS device to track a vehicle's movements for nearly a month violated Jones's reasonable expectation of privacy”).

Furthermore, Justice Alito's opinion, in which three other Justices joined, does

¹⁴ Notably, each of these approaches also differs from the court of appeals' methodology, which, as discussed above, focused on whether Jones' movements over nearly a month would have been observed by a single member of the public. See Maynard, 615 F.3d at 560.

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

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

not mention Smith at all. See Jones, 132 S. Ct. at 957-64 (Alito, J., concurring in the judgment). And although Justice Sotomayor stated in her concurring opinion that "it may be necessary to reconsider" the third-party disclosure principle applied in Smith and Miller, which she described as "ill suited to the digital age," she expressly stated that it was unnecessary for the Court to undertake such a reexamination in Jones. See id. at 957 (Sotomayor, J., concurring) ("Resolution of these difficult questions in this case is unnecessary . . . because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision.").¹⁵

¹⁵ Both the opinion of the Supreme Court in Jones and Justice Sotomayor's concurring opinion mention a brief passage in Knotts reserving the question whether the tracking of a person's location might become so pervasive or abusive as to require a different approach. See Jones, 132 S. Ct. at 952 n.6; id. at 956 n.* (Sotomayor, J., concurring). The respondent in Knotts had argued that "the result of a ruling for the Government will be that 'twenty-four hour surveillance of any citizen of this country will be possible without judicial knowledge or supervision.'" Knotts, 460 U.S. at 283 (quoting Brief for Respondent). In response, the Supreme Court asserted that "the 'reality hardly suggests abuse,'" and that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Id. (quoting Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).

Contrary to Judge Leon's conclusion, see Klayman, 957 F. Supp. 2d at 31-32 & n.46, this passage from Knotts also fails to support his decision to depart from Smith. Unlike Knotts (and Jones), this matter does not involve the electronic tracking of location at all, much less the sort of "twenty-four hour" tracking envisioned by the respondent in Knotts. Instead, this case, like Smith, involves the production of call detail records created by the phone company based on data submitted to it by callers.

(continued...)

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

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

Smith directly applies to the call detail records produced as part of the NSA telephony metadata program and remains binding even after Jones. Judge Leon's efforts to distinguish Smith are unpersuasive, and his analysis in Klayman is also difficult to reconcile with other Supreme Court decisions, such as Rakas and Carter, which, as discussed above, hold that Fourth Amendment rights are personal and cannot be vicariously asserted. The broader adoption of Judge Leon's approach would raise numerous difficult questions requiring the reexamination of a range of settled Fourth Amendment precedents. See Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Mich. L. Rev. at 328-43; see also Jones, 132 S. Ct. at 954 (asserting that Justice Alito's expectation-of-privacy analysis would lead to "thorny problems").¹⁶ Any such overhaul

¹⁵(...continued)

Smith, which is directly applicable to such information, does not state or suggest that application of the third-party disclosure principle depends upon the quantity of dialing information disclosed by a caller or turned over the Government. Indeed, any such statement or suggestion would be contrary to the logic of the decision – that by voluntarily disclosing dialing information to the phone company, a caller forfeits any legitimate expectation of privacy therein. Smith, 442 U.S. at 744 (citing Miller, 425 U.S. at 442-44)).

¹⁶ A threshold question is which standard should govern; as discussed above, the court of appeals' decision in Maynard and the two concurrences in Jones suggest three different standards. See Kerr, "The Mosaic Theory of the Fourth Amendment," 111 Mich. L. Rev. at 329. Another question is how to group Government actions in assessing whether the aggregate conduct constitutes a search. See *id.* For example, "[w]hich surveillance methods prompt a mosaic approach? Should courts group across
(continued...)

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

Page 29

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

of Fourth Amendment law is for the Supreme Court, rather than this Court, to initiate.

While the concurring opinions in Jones may signal that some or even most of the

Justices are ready to revisit certain settled Fourth Amendment principles, the decision in

Jones itself breaks no new ground concerning the third-party disclosure doctrine

generally or Smith specifically. The concurring opinions notwithstanding, Jones simply

cannot be read as inviting the lower courts to rewrite Fourth Amendment law in this

area. This Court concludes that where the acquisition of non-content call detail records

such as dialing information is concerned, Smith remains controlling.¹⁷

III. CONCLUSION

For the foregoing reasons, [REDACTED] asks this Court to modify or set aside the Secondary Order issued to it on January 3, 2014, the Petition is denied.

¹⁶(...continued)

surveillance methods? If so, how?" Id. Still another question is how to analyze the reasonableness of mosaic searches, which "do not fit an obvious doctrinal box for determining reasonableness." Id. Courts adopting a mosaic theory would also have to determine whether, and to what extent, the exclusionary rule applies: Does it "extend over all of the mosaic or only the surveillance that crossed the line to trigger a search?" Id. at 329-30.

¹⁷ Because this Court concludes that Smith is controlling and that the telephony metadata program involves no search under the Fourth Amendment, the Court need not address the question of reasonableness. See Klayman, 957 F. Supp. 2d at 37-42 (holding that plaintiffs are likely to succeed in showing searches that Judge Leon concluded are effected by NSA telephony metadata program are unreasonable).

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

Page 30

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

Pursuant to 50 U.S.C. § 1861(f)(2)(B), the Secondary Order is affirmed, [REDACTED] is directed to continue to comply with the Secondary Order until it expires by its own terms.

Since last summer, the Government has declassified and made public substantial details regarding the NSA telephony metadata program. Among other things, substantial portions of this Court's January 3 Primary Order and all predecessor orders have been publicly released. In light of those disclosures and the ongoing public debate regarding this program, both the Government [REDACTED] submit memoranda (or a joint memorandum) stating their views with respect to whether this Court can or should unseal the Petition, the Government's Response, and this Opinion and Order, and whether appropriately redacted versions of these documents should be published pursuant to FISC Rule 62(a). Such memoranda are to be submitted, under seal, no later than 5:00 p.m. Eastern Time on April 10, 2014.

SO ORDERED, this 20th day of March, 2014.


ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

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

Page 31

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, <i>et al.</i> ,)	
)	
Plaintiffs,)	
)	
v.)	Civil Action No.
)	1:13-cv-0851-RJL
BARACK OBAMA, President of the United States, <i>et al.</i> ,)	
)	
Defendants.)	

DECLARATION OF TERESA H. SHEA, SIGNALS INTELLIGENCE
DIRECTOR, NATIONAL SECURITY AGENCY

I, Teresa H. Shea, for my declaration in the above-captioned case, do hereby state and declare as follows:

1. I am the Director of the Signals Intelligence Directorate (SID) at the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for, among other things, protecting NSA Signals Intelligence (SIGINT) activities, sources, and methods against unauthorized disclosures.

2. I submit this declaration to discuss the transition ordered by the President to the NSA's bulk telephony metadata program (carried out under Section 215 of the USA-PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)) to preserve the program's needed capabilities while enhancing the program's protections against the potential for abuse. I also address certain speculation about the program's scope. My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, and the information available to me in my capacity as SIGINT Director.

**TRANSITION TO THE SECTION 215 TELEPHONY METADATA
PROGRAM ORDERED BY THE PRESIDENT**

3. On January 17, 2014, following a review of the Nation's Signals Intelligence programs, the President announced a series of reforms designed to preserve the Intelligence Community's capabilities to detect and prevent threats by foreign terrorist organizations through the penetration of their communications, while enhancing protections for individual privacy as intelligence capabilities developed to meet the threat of international terrorism continue to advance. A transcript of the President's remarks is available at <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.

4. Regarding the Section 215 telephony metadata program, the President ordered a transition during which the Intelligence Community and the Attorney General were to develop options for a new approach that can match the program's capabilities without the Government continuing to hold the bulk telephony metadata. The President also directed: (1) that the Government work with the Foreign Intelligence Surveillance Court (FISC) to require, during the transition period, advance findings by FISC judges of "reasonable, articulable suspicion" that selectors (such as telephone numbers) used to query the database are associated with foreign terrorist organizations (except in emergency situations, in which case FISC approval is to be sought retrospectively); and (2) that query results available to NSA analysts be limited to metadata within two "hops" (degrees of contact) of suspected terrorist selectors, not three as previously allowed.

5. The Government (including NSA) took immediate steps to put these two changes into effect. Among these steps, the Government filed a motion with the FISC to amend its January 3, 2014, Primary Order approving the Section 215 telephony metadata program. The Government's motion proposed two changes to the previously approved minimization procedures: First, the Government proposed a change that (except in cases of emergency) would

require it to obtain permission from the FISC to use a proposed selector as a “seed” to query the telephony metadata, based on a finding by the FISC that the selector to be used satisfies the “reasonable, articulable suspicion” standard. Second, the Government proposed limiting the results of each query to metadata that are within two, rather than three, “hops” of the approved selector used to conduct the query. On February 5, 2014, the FISC granted the Government’s motion to implement these two changes to the Section 215 program. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR14-01 (F.I.S.C. Feb. 5, 2014) (publicly released, unclassified version) (Enclosure A).

6. On March 27, 2014, the President announced that, after having considered options presented to him by the Intelligence Community and the Attorney General, he will seek legislation to replace the Section 215 telephony metadata program. Statement by the President on the Section 215 Bulk Metadata Program, <http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program>. The President stated that his goal is to “establish a mechanism to preserve the capabilities we need without the Government holding this bulk metadata” to “give the public greater confidence that their privacy is appropriately protected,” while maintaining the intelligence tools needed “to keep us safe.” Instead of the Government obtaining business records of telephony metadata in bulk, the President proposed that telephony metadata should remain in the hands of telecommunications companies. The President stated that “legislation will be needed to permit the Government to obtain information with the speed and in the manner that will be required to make this approach workable.” Under such legislation, the Government would be authorized to obtain telephony metadata from the companies pursuant to individualized orders from the FISC. The President explained that, in the meantime, the Government would seek from the FISC a 90-day

reauthorization of the existing Section 215 program, with the two modifications already approved by the FISC in February.

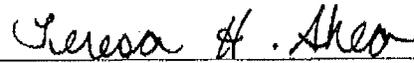
7. On March 28, 2014, the FISC issued a new Primary Order approving the Government's application to reauthorize the program, with the modifications described above, for approximately another 90 days (through June 20, 2014). The FISC's action brought to 37 the number of times the FISC (by 16 different judges) has authorized the NSA's bulk collection of telephony metadata under Section 215 of the USA-PATRIOT Act.

SCOPE OF THE SECTION 215 TELEPHONY METADATA PROGRAM

8. Although there has been speculation that the NSA, under this program, acquires metadata relating to all telephone calls to, from, or within the United States, that is not the case. The Government has acknowledged that the program is broad in scope and involves the collection and aggregation of a large volume of data from multiple telecommunications service providers, but as the FISC observed in a decision last year, the program has never captured information on all (or virtually all) calls made and/or received in the U.S. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR13-109, Amended Mem. Op. at 4 n.5 (F.I.S.C. Aug. 29, 2013) (public unclassified version) ("The production of all call detail records of all persons in the United States has never occurred under this program."). And while the Government has also acknowledged that one provider was the recipient of a now-expired April 25, 2013, Secondary Order from the FISC, the identities of the carriers participating in the program (either now, or at any other time) otherwise remain classified.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: May 1, 2014



Teresa H. Shea
Signals Intelligence Director
National Security Agency

No. 14-35555

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ANNA J. SMITH

Plaintiff-Appellant,

v.

BARACK OBAMA et al.,

Defendant-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT
COURT FOR THE DISTRICT OF IDAHO

SUPPLEMENTAL EXCERPTS OF RECORD

JOYCE R. BRANDA
*Acting Assistant Attorney
General*

WENDY J. OLSON
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
HENRY C. WHITAKER
*(202) 514-3180
Attorneys, Appellate Staff
Civil Division, Room 7256
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530*

TABLE OF CONTENTS

Court Record No.	Document Description	SER Page No.
DE 8	Plaintiff's Motion for a Preliminary Injunction	1
DE 15-2	Declaration of Teresa H. Shea (Jan. 24, 2014)	4
DE 15-4	Foreign Intelligence Surveillance Court Opinion (Aug. 29, 2013)	28
DE 15-5	Foreign Intelligence Surveillance Court Opinion (Oct. 11, 2013)	74
DE 15-8	President's January 17, 2014 Statement	97
DE 15-11	Report on NSA's Bulk Collection Programs Affected by USA PATRIOT ACT Reauthorization (2009)	105
DE 15-14	Report on NSA's Bulk Collection Programs Affected by USA PATRIOT ACT Reauthorization (2011)	110
DE 15-7	Secondary Order	115

PETER J. SMITH IV, ISB 6997
Lukins & Annis, P.S.
601 E. Front Avenue, Suite 502
Coeur d’Alene, ID 83814
Phone: 208-667-0517
Fax: 208-664-4125
Email: psmith@lukins.com

LUCAS T. MALEK, ISB 8610
Luke Malek, Attorney at Law, PLLC
721 N 8th Street
Coeur d’Alene, ID 83814
Phone: 208-661-3881
Email: Luke_Malek@hotmail.com

Attorneys for the Plaintiff ANNA J. SMITH

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

ANNA J. SMITH,

Plaintiff,

vs.

BARACK H. OBAMA, in his official capacity as President of the United States of America; JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

CASE NO. 2:13-cv-00257

PLAINTIFF’S MOTION FOR PRELIMINARY INJUNCTION

Upon pleadings and papers in this matter, Plaintiff moves this Court before the Honorable Ronald E. Bush, United States District Court Judge, at the United States Courthouse – Northern Division – 6450 N. Mineral Drive, Coeur d’Alene, Idaho 83815, for a preliminary injunction against the Defendants, their agents, servants, employees, officials, or any other person acting in concert with them or on their behalf, pursuant to Rule 65 of the Federal Rules of Civil Procedure.

In particular, Plaintiff move this Court for a preliminary injunction that, during the pendency of this suit, (i) bars Defendants from collecting Plaintiff’s call records under the mass call-tracking program, (ii) requires Defendants to quarantine all of Plaintiff’s call records already collected under the program, and (iii) prohibits Defendants from querying metadata obtained through the program using any phone number or other identifier associated with Plaintiff.

As set forth in the accompanying memorandum of law and declarations in support of this motion, and in the Complaint, Plaintiff meets all of the requirements for the issuance of a preliminary injunction. Specifically, Plaintiff submits:

1. Memorandum in Support of Plaintiff’s Motion for Preliminary Injunction;
2. Declaration of Anna J. Smith; and
3. Declaration of Peter J. Smith IV.

Oral argument is requested.

DATED this 20th day of December, 2013.



PETER J. SMITH IV, ISB 6997
Co-Counsel for Plaintiff
ANNA J. SMITH

CERTIFICATE OF SERVICE

I hereby certify that on this 20th day of December, 2013, I served a true and correct copy of the foregoing PLAINTIFF’S MOTION FOR PRELIMINARY INJUNCTION by the method described below to:

JAMES J. GILLIGAN	<input type="checkbox"/>	U.S. Mail
Special Litigation Counsel	<input type="checkbox"/>	Hand Delivered
U.S Department of Justice Civil Division	<input type="checkbox"/>	Overnight Mail
Federal Programs Branch	<input type="checkbox"/>	Telecopy (FAX) (202) 616-8470
20 Massachusetts Ave., N.W., Room 6102	<input checked="" type="checkbox"/>	Electronic Mail james.gilligan@usdoj.gov
Washington, D.C. 20001		

MARCIA BERMAN	<input type="checkbox"/>	U.S. Mail
Senior Trial Counsel	<input type="checkbox"/>	Hand Delivered
U.S Department of Justice Civil Division	<input type="checkbox"/>	Overnight Mail
Federal Programs Branch	<input type="checkbox"/>	Telecopy (FAX) (202) 616-8470
20 Massachusetts Ave., N.W., Room 7132	<input checked="" type="checkbox"/>	Electronic Mail marcia.berman@usdoj.gov
Washington, D.C. 20001		

RODNEY PATTON	<input type="checkbox"/>	U.S. Mail
Trial Attorney	<input type="checkbox"/>	Hand Delivered
U.S Department of Justice Civil Division	<input type="checkbox"/>	Overnight Mail
Federal Programs Branch	<input type="checkbox"/>	Telecopy (FAX) (202) 616-8470
20 Massachusetts Ave., N.W., Room 7320	<input checked="" type="checkbox"/>	Electronic Mail rodney.patton@usdoj.gov
Washington, D.C. 20001		

SYRENA C. HARGROVE	<input type="checkbox"/>	U.S. Mail
Assistant United States Attorney	<input type="checkbox"/>	Hand Delivered
District of Idaho	<input type="checkbox"/>	Overnight Mail
Washington Group Plaza Iv	<input type="checkbox"/>	Telecopy (FAX) (208) 334-1414
800 E. Park Boulevard, Suite 600	<input checked="" type="checkbox"/>	Electronic Mail Syrena.Hargrove@usdoj.gov
Boise, ID 83712-9903		

PJS

STUART F. DELERY
 Assistant Attorney General
 JOSEPH H. HUNT
 Director, Federal Programs Branch
 ANTHONY J. COPPOLINO
 Deputy Branch Director
 tony.coppolino@usdoj.gov
 JAMES J. GILLIGAN
 Special Litigation Counsel
 james.gilligan@usdoj.gov
 MARCIA BERMAN
 Senior Trial Counsel
 marcia.berman@usdoj.gov
 BRYAN DEARINGER
 Trial Attorney
 bryan.dearinger@usdoj.gov
 RODNEY PATTON
 Trial Attorney
 rodney.patton@usdoj.gov
 U.S. Department of Justice, Civil Division
 20 Massachusetts Avenue, NW, Rm. 7132
 Washington, D.C. 20001
 Phone: (202) 514-2205; Fax: (202) 616-8471

WENDY OLSON, Idaho Bar No. 7634
 United States Attorney
 SYRENA C. HARGROVE, Idaho Bar No. 6213
 Assistant United States Attorney
 District of Idaho
 Washington Group Plaza IV
 800 E. Park Boulevard, Suite 600
 Boise, ID 83712-9903
 Telephone: (208) 334-1211
 Facsimile: (208) 334-1414
 Syrena.Hargrove@usdoj.gov

Attorneys for the Government Defs. in their Official Capacity

**IN THE UNITED STATES DISTRICT COURT
 FOR THE DISTRICT OF IDAHO**

)	Case No. 2:13-cv-00257
ANNA J. SMITH)	
)	
Plaintiff,)	DECLARATION OF TERESA H.
)	SHEA, SIGNALS
v.)	INTELLIGENCE DIRECTOR,
)	NATIONAL SECURITY
BARACK H. OBAMA, <i>et al.</i> ,)	AGENCY
)	
Defendants.)	
)	

I, Teresa H. Shea, do hereby state and declare as follows:

(U) Introduction and Summary

1. I am the Director of the Signals Intelligence Directorate (SID) at the National Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for the collection, processing, and dissemination of Signals Intelligence (SIGINT) information for the foreign intelligence purposes of the U.S. I have been designated an original TOP SECRET classification authority under Executive Order (E.O.) 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information Security Program (Feb. 24, 2012).

2. My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, the information available to me in my capacity as SIGINT Director, and the advice of counsel.

3. The NSA was established by Presidential Directive in 1952 as a separately organized agency within the DOD under the direction, authority, and control of the Secretary of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate SIGINT information for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) to support national and departmental missions. See E.O. 12333, section 1.7(c), as amended.

4. The NSA's responsibilities include SIGINT, i.e., the collection, processing and dissemination of intelligence information from certain signals for foreign intelligence and

counterintelligence purposes and to support military operations, consistent with U.S. laws and the protection of privacy and civil liberties. In performing its SIGINT mission, the NSA exploits foreign electromagnetic signals, communications, and information about communications to obtain intelligence information necessary to national defense, national security, or the conduct of foreign affairs. The NSA has developed a sophisticated worldwide SIGINT collection network that acquires foreign and international electronic communications. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and a remarkable amount of human effort. It relies on sophisticated collection and processing technology.

5. I discuss herein an NSA intelligence collection program involving the acquisition and analysis of telephony metadata. I also discuss the transition recently ordered by the President to preserve the program's needed capabilities while enhancing the program's protections against the potential for abuse. Although the existence of the program has been publicly acknowledged by the Government, numerous details about its scope and operation remain classified, and cannot be revealed in a public declaration. I therefore limit my discussion herein to facts about the program and its value as an intelligence tool that are unclassified in nature. As explained below, plaintiff's preliminary injunction motion and complaint inaccurately describe the program. While the NSA obtains telephony metadata in bulk from certain telecommunications service providers, the NSA's use of that data is strictly controlled; only a very small percentage of the total data collected is ever reviewed by intelligence analysts; and results of authorized queries can be further analyzed and disseminated for valid counterterrorism purposes.

OVERVIEW OF PROGRAM

6. One of the greatest challenges the U.S. 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 U.S. Detecting and preventing threats by exploiting terrorist communications has been, and continues to be, one of the tools in this effort. It is imperative that we have the capability to rapidly detect any terrorist threat inside the U.S.

7. One method that the NSA has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the U.S. The term “telephony metadata” or “metadata” as used here refers to data collected under the program that are about telephone calls—such as the initiating and receiving telephone numbers, and the time and duration of the calls—but does not include the substantive content of those calls or any subscriber identifying information.

8. By analyzing telephony metadata based on telephone numbers associated with terrorist activity, trained expert intelligence analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the U.S.

9. Foreign terrorist organizations use the international telephone system to communicate with one another between numerous countries all over the world, including calls to and from the U.S. When they are located inside the U.S., terrorist operatives also make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the U.S., or those that are purely domestic, because those communications are particularly likely to identify suspects in the U.S. whose activities may include planning attacks against the homeland.

10. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting such communications between known or suspected terrorists who are operating outside of the U.S. and who are communicating with others inside the U.S., as well as communications between operatives who are located within the U.S.

11. Detecting and linking these types of communications was identified as a critical intelligence gap in the aftermath of the September 11, 2001 attacks. One striking example of this gap is that, prior to those attacks, the NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, then living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using overseas signals intelligence capabilities, but those capabilities did not capture the calling party's telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysis mistakenly concluded that al-Mihdhar was overseas and not in California. Telephony metadata of the type acquired under this program, however, would have included the missing information and might have permitted NSA intelligence analysts to tip FBI to the fact that al-Mihdhar was calling the Yemeni safe house from a U.S. telephone identifier.

12. The utility of analyzing telephony metadata as an intelligence tool has long been recognized. As discussed below, experience also shows that telephony metadata analysis in fact produces information pertinent to FBI counterterrorism investigations, and can contribute to the prevention of terrorist attacks.

13. Since May 2006, pursuant to orders obtained from the Foreign Intelligence Surveillance Court ("FISC"), under the "business records" provision of the Foreign Intelligence Surveillance Act ("FISA"), enacted by Section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861 (Section 215), NSA has collected and analyzed bulk telephony metadata from

certain telecommunications service providers to address the intelligence gap that allowed al-Mihdhar to operate undetected within the U.S. while communicating with a known terrorist overseas.

14. Pursuant to Section 215, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce all business records created by them (known as call detail records) that contain information about communications between telephone numbers, generally relating to telephone calls made between the U.S. and a foreign country and calls made entirely within the U.S. As the FISC has recently observed, the production of all call detail records of all persons in the U.S. has never occurred under this program. By their terms, these FISC orders must be renewed approximately every 90 days. Redacted, declassified versions of a recent FISC “Primary Order” and “Secondary Order,” directing certain telecommunications service providers to produce telephony metadata records to NSA, and imposing strict conditions on the Government’s access to and use and dissemination of the data, are attached, respectively, as Exhibits A and B hereto. At least 15 different FISC judges have entered a total of 36 orders authorizing NSA’s bulk collection of telephony metadata under Section 215, most recently on January 3, 2014.

15. Under the terms of the FISC’s orders, the information the Government is authorized to collect includes, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call. The FISC’s orders authorizing the collection do not allow the Government to collect the content of any telephone call, nor the names, addresses, or financial information of parties to any call. The metadata collected by the

Government pursuant to these orders also does not include cell site locational information.

16. The NSA, in turn, stores and analyzes this information under carefully controlled circumstances, and refers to the FBI information about communications (e.g., telephone numbers, dates of calls, etc.) that the NSA concludes have counterterrorism value, typically information about communications between known or suspected terrorist operatives and persons located within the U.S.

17. Although it is popularly assumed that the NSA, under this program, acquires metadata relating to all telephone calls to, from, or within the United States, that is not the case, as the FISC recently observed. As the Government has acknowledged, the program is broad in scope and involves the collection and aggregation of a large volume of data from multiple telecommunications service providers, but it has never captured information on all (or virtually all) calls made and/or received in the U.S. And while the Government has also acknowledged that one provider was the recipient of a now-expired April 25, 2013, Secondary Order from the FISC (Exhibit B, attached), the identities of the carriers participating in the program (either now, or at any time in the past) otherwise remain classified.

18. Under the FISC's orders, the Government is prohibited from accessing the metadata for any purpose other than obtaining counterterrorism information relating to telephone numbers (or other identifiers) that are reasonably suspected of being associated with specific foreign terrorist organizations or rendering the metadata useable to query for such counterterrorism related information.

19. Pursuant to Section 215 and the FISC's orders, the NSA does not itself in the first instance record any metadata concerning anyone's telephone calls. Nor is any non-governmental party required by Section 215, the FISC or the NSA to create or record the information that the

NSA obtains pursuant to Section 215 and FISC orders. Rather, pursuant to the FISC's orders, telecommunications service providers turn over to the NSA business records that the companies already generate and maintain for their own pre-existing business purposes (such as billing and fraud prevention).

QUERY AND ANALYSIS OF METADATA

20. Under the FISC's orders authorizing the NSA's bulk collection of telephony metadata, the NSA may access the data for purposes of obtaining counterterrorism information only through queries (term searches) using metadata "identifiers," e.g., telephone numbers, that are associated with a foreign terrorist organization.

21. Specifically, under the terms of the FISC's Primary Order, before an identifier may be used to query the database there must be a "reasonable articulable suspicion" (RAS), based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, that the identifier is associated with one of the identified international terrorist organizations that are subjects of FBI counterterrorism investigations. The RAS requirement ensures an ordered and controlled querying of the collected data; it is also designed to prevent any general browsing of data. Further, when the identifier is reasonably believed to be used by a U.S. person, the suspicion of association with a foreign terrorist organization cannot be based solely on activities protected by the First Amendment. An identifier used to commence a query of the data is referred to as a "seed."

22. Information responsive to an authorized query could include 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. Query results do not include the identities of the individuals

associated with the responsive telephone numbers, because that is subscriber information that is not included in the telephony metadata.

23. Under the FISC's orders issued from May 2006 to January 3, 2014, the NSA has also been permitted to obtain information concerning second and third-tier contacts of the identifier, also known as "hops." The first "hop" refers to the set of identifiers directly in contact with the seed identifier. The second "hop" refers to the set of identifiers found to be in direct contact with the first "hop" identifiers, and the third "hop" refers to the set of identifiers found to be in direct contact with the second "hop" identifiers. In accordance with the recent instruction of the President, discussed below, the NSA has taken immediate steps to implement restrictions limiting its review of queries to two "hops" only and the Government is now working with the FISC to incorporate this restriction into the FISC's orders.

24. Although bulk metadata are consolidated and preserved by the NSA pursuant to Section 215, the vast majority of that information is never seen by any person. Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated by NSA intelligence analysts, and only under carefully controlled circumstances. Likewise, only a tiny fraction of the records are reviewed by technical personnel in the process of rendering the data usable for query purposes.

25. For example, although the number of unique identifiers has varied over the years, in 2012, fewer than 300 met the RAS 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 at multiple "hops" from the seed identifier, the number of metadata records responsive to such queries is

substantially larger than 300, but it is still a very small percentage of the total volume of metadata records.

26. There is no typical number of records responsive to a query of the metadata—the number varies widely depending on how many separate telephone numbers (or other identifiers) the “seed” identifier has been in direct contact with, how many separate identifiers those in the first-tier contact, and so forth.

27. The NSA does not disseminate metadata information that it has not determined to be of counterterrorism value, regardless of whether it was obtained at the first, second, or third hop from a seed identifier. Rather, NSA intelligence analysts work to ascertain which of the results are likely to contain foreign intelligence information related to counterterrorism that would be of investigative value to the FBI (or other intelligence agencies). For example, analysts may rely on SIGINT or other intelligence information available to them, or chain contacts within the query results themselves, to inform their judgment as to what information should be passed to the FBI as leads or “tips” for further investigation. As a result, during the three-year period extending from May 2006 (when the FISC first authorized NSA’s telephony metadata program under Section 215) through May 2009, NSA provided to the FBI and/or other intelligence agencies a total of 277 reports containing approximately 2,900 telephone identifiers that the NSA had determined to be of investigative value.

28. It is not accurate, therefore, to suggest that the NSA can or does “track,” “monitor,” or “search” all Americans’ calls or that it engages in “surveillance,” under Section 215. Rather, by the terms of the FISC’s orders, the NSA has been permitted only to access metadata information within, at most, three “hops” of an approved seed identifier that is reasonably suspected of being associated with a foreign terrorist organization specified in the FISC’s orders.

29. Even when the NSA conducts authorized queries of the database, it does not use the results to provide the FBI, or any other agency, with complete profiles on suspected terrorists or comprehensive records of their associations. Rather, the NSA applies the tools of SIGINT analysis to focus only on those identifiers which, based on the NSA's experience and judgment, and other intelligence available to it, may be of use to the FBI in detecting persons in the U.S. who may be associated with a specified foreign terrorist organization and acting in furtherance of their goals. Indeed, under the FISC's orders, the NSA is prohibited from disseminating any U.S.-person information derived from the metadata unless one of a very limited number of senior NSA officials determines that the information is in fact related to counterterrorism information, and is necessary to understand the counterterrorism information or assess its importance. The NSA disseminates no information derived from the metadata about persons whose identifiers have not been authorized as query terms under the RAS standard, or whose metadata are not responsive to other queries authorized under that standard.

MINIMIZATION PROCEDURES AND OVERSIGHT

30. The NSA's access to, review, and dissemination of telephony metadata collected under Section 215 is subject to rigorous procedural, technical, and legal controls, and receives intensive oversight from numerous sources, including frequent internal NSA audits, Justice Department and Office of the Director of National Intelligence (ODNI) oversight, and reports to the FISC and to the Congressional intelligence committees.

31. In accordance with the requirements of Section 215, "minimization procedures" are in place to guard against inappropriate or unauthorized dissemination of information relating to U.S. persons. First among these procedures is the requirement that the NSA store and process the metadata in repositories within secure networks, and that access to the metadata be permitted

only for purposes allowed under the FISC's order, specifically database management and authorized queries for counterterrorism purposes under the RAS standard. In addition, the metadata must be destroyed no later than five years after their initial collection.

32. Second, under the FISC's orders issued from May 2006 to January 3, 2014, no one other than twenty-two designated officials in the NSA's Homeland Security Analysis Center and the Signals Intelligence Directorate could make findings of RAS that a proposed seed identifier is associated with a specified foreign terrorist organization. For identifiers believed to be associated with U.S. persons, the NSA's Office of General Counsel must also determine that a finding of RAS is not based solely on activities protected by the First Amendment. And, as noted above, the minimization requirements ordered by the FISC also limit the results of approved queries to metadata within three hops of the seed identifier while, pursuant to the President's direction, the NSA has taken immediate steps to implement restrictions limiting its review of queries to two "hops" only and the Government is now working with the FISC to incorporate this restriction into the FISC's orders.

33. Third, while the results of authorized queries of the metadata may be shared, without minimization, among trained NSA personnel for analysis purposes, no results may be disseminated outside of the NSA except in accordance with the minimization and dissemination requirements and established NSA procedures. Moreover, prior to dissemination of any U.S. person information outside of the NSA, one of a very limited number of NSA officials must determine that the information is in fact related to counterterrorism information, and is necessary to understand the counterterrorism information or assess its importance.

34. Fourth, in accordance with the FISC's orders, the NSA has imposed stringent and mutually reinforcing technological and personnel training measures to ensure that queries will be

made only as to identifiers about which RAS has been established. These include requirements that intelligence analysts receive comprehensive training on the minimization procedures applicable to the use, handling, and dissemination of the metadata, and technical controls that prevent NSA intelligence analysts from seeing any metadata unless as the result of a query using an approved identifier.

35. Fifth, 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. Among these additional safeguards and requirements are audits and reviews of various aspects of the program, including RAS findings, by several entities within the Executive Branch, including the 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.

36. Finally, in addition to internal oversight, any compliance matters in the program identified by the NSA, DOJ, or ODNI are reported to the FISC. Applications for 90-day renewals must report information on how the NSA's authority to collect, store, query, review and disseminate telephony metadata was implemented under the prior authorization. Significant compliance incidents are also reported to the Intelligence and Judiciary Committees of both houses of Congress.

TRANSITION ORDERED BY THE PRESIDENT

37. On January 17, 2014, following a review of the Nation's signals intelligence programs, the President announced a series of reforms designed to preserve the Intelligence Community's capabilities to detect and prevent threats by foreign terrorist organizations through the penetration of their communications, while enhancing protections for individual privacy as

intelligence capabilities developed to meet the threat of international terrorism continue to advance. (A transcript of the President's remarks is available at <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>).

38. Regarding the bulk telephony metadata program, the President ordered a transition during which the Intelligence Community and the Attorney General are to develop options for a new approach that can match the program's capabilities without the Government continuing to hold the bulk telephony metadata itself. The President also directed that, effectively immediately: (1) the NSA will access only those identifiers within two "hops" of a seed identifier—not three—when querying the database; and (2) the Government will work with the FISC so that, during the transition period, findings of "reasonable, articulable suspicion" that proposed seed identifiers are associated with foreign terrorist organizations will be made by the FISC, rather than NSA officials, except in cases of true emergency. In accordance with the President's instruction, the NSA has taken immediate steps to implement restrictions limiting its review of queries to two "hops" only and the Government is now working with the FISC to incorporate this restriction into the FISC's orders. Additionally, the Government is now working with the FISC to require that during the transition ordered by the President, the NSA obtain the FISC's permission before the NSA may use proposed identifiers to query the database, except in cases of emergency.

COMPLIANCE INCIDENTS

39. Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues (described below) that were discovered as a result of internal NSA oversight and of DOJ and ODNI reviews. Upon

discovery, these violations were reported by the Government to the FISC and Congress, the NSA remedied the problems, and the FISC reauthorized the program.

40. For example, beginning in mid-January 2009, the Government notified the FISC that the NSA employed an “alert list” consisting of counterterrorism telephony identifiers to provide automated notification to signals intelligence analysts if one of their assigned foreign counterterrorism targets was in contact with a telephone identifier in the U.S., or if one of their targets associated with foreign counterterrorism was in contact with a foreign telephone identifier. The NSA’s process compared the telephony identifiers on the alert list against incoming Section 215 telephony metadata as well as against telephony metadata that the NSA acquired pursuant to its Executive Order 12333 SIGINT authorities. Reports filed with the FISC incorrectly stated that each of the telephone identifiers the NSA placed on the alert list had been determined, through the RAS process, to be reasonably associated with a foreign terrorist organization as required by the FISC’s orders. In fact, however, the majority of telephone identifiers included on the alert list had not gone through the process of becoming RAS approved, even though the identifiers were suspected of being associated with a foreign terrorist organization. The NSA shut down the automated alert list process and corrected the problem.

41. Following this notification, the Director of the NSA ordered an end-to-end system engineering and process review of its handling of the Section 215 metadata. On March 2, 2009, the FISC ordered the NSA to seek FISC approval to query the Section 215 metadata on a case-by-case basis, except where necessary to protect against an imminent threat to human life. The FISC further ordered the NSA to file a report with the FISC following the completion of the end-to-end review discussing the results of the review and any remedial measures taken. The report filed by the NSA discussed all of the compliance incidents, some of which involved queries of

the Section 215 metadata using non-RAS approved telephone identifiers, and how they had been remedied. The compliance incidents, while serious, generally involved human error or complex technology issues related to the NSA's compliance with particular aspects of the FISC's orders. Subsequently, the FISC required a full description of any incidents of dissemination outside of the NSA of U.S. person information in violation of court orders, an explanation of the extent to which the NSA had acquired foreign-to-foreign communications metadata pursuant to the court's orders and whether the NSA had complied with the terms of court orders in connection with any such acquisitions, and certification as to the status of several types of data to the extent those data were collected without authorization.

42. The U.S. Government completed these required reviews and reported to the FISC in August 2009. In September 2009, the FISC entered an order permitting the NSA to once again assess RAS without seeking pre-approval from the FISC subject to the minimization and other requirements that remain in place today. As noted above, the Government is now working with the FISC to require that during the transition ordered by the President, the NSA obtain the FISC's permission before the NSA may use proposed identifiers to query the database, except in cases of emergency.

43. In fact, in an August 2013 Amended Memorandum Decision discussing the Court's reasons for renewing the continued operation of the Section 215 telephony metadata program for a 90-day period, the FISC stated, "The Court is aware that in prior years there have been incidents of non-compliance with respect to the NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved." *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*, Case No. BR 13-109, Amended Memorandum Opinion at 5

n.8 (FISC, released in redacted form September 17, 2013; *available at* <http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf> (last visited December 2, 2013)).

44. These incidents, including the FISC's related opinions, were also reported to Congress in 2009.

45. Having received these reports and having been informed that the Government interpreted Section 215 to authorize the bulk collection of telephony metadata, Congress has twice reauthorized Section 215, without relevant modification, in 2010 and again in 2011.

46. In sum, the factors giving rise to compliance incidents discussed in this section have been remedied. Moreover, even the most serious incidents, in which non-RAS approved selectors were used to query the database, would not have allowed the NSA to draw a "detailed picture" of the persons with whom an individual interacts, as plaintiff speculates. That type of analysis is simply not possible from the raw telephony metadata that is collected under the program, as it does not identify who is calling whom and for what purpose.

BENEFITS OF METADATA COLLECTION

47. Among other benefits, the bulk collection of telephony metadata under Section 215 has an important value to NSA intelligence analysts tasked with identifying potential terrorist threats to the U.S. homeland, in support of FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks both in the U.S. and abroad. By applying the FISC-ordered RAS standard to telephone identifiers used to query the metadata, NSA intelligence analysts are able to: (i) detect domestic identifiers calling foreign identifiers associated with one of the foreign terrorist organizations and discover identifiers that the foreign identifiers are in contact with; (ii) detect foreign identifiers associated with a foreign terrorist

organization calling into the U.S. and discover which domestic identifiers are in contact with the foreign identifiers; and (iii) detect possible terrorist-related communications occurring between communicants located inside the U.S.

48. Although the NSA possesses a number of sources of information that can each be used to provide separate and independent indications of potential terrorist activity against the U.S. and its interests abroad, the best analysis occurs when NSA intelligence analysts can consider the information obtained from each of those sources together to compile and disseminate to the FBI as complete a picture as possible of a potential terrorist threat. While telephony metadata is not the sole source of information available to NSA counterterrorism personnel, it provides a component of the information NSA intelligence analysts rely upon to execute this threat identification and characterization role.

49. An advantage of bulk metadata analysis as applied to telephony metadata, which is interconnected in nature, is that it enables the Government to quickly analyze past connections and chains of communication. Unless the data is aggregated, it may not be feasible to detect chains of communications that cross communication networks. The ability to query accumulated telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations who might otherwise go undetected.

50. Specifically, when the NSA performs a contact-chaining query on a terrorist associated telephone identifier, it is able to detect not only the further contacts made by that first tier of contacts, but the additional tiers of contacts, out to the maximum number of permitted "hops" from the original identifier. The collected metadata thus holds contact information that can be immediately accessed as new terrorist-associated telephone identifiers are identified. Multi-tiered contact chaining identifies not only the terrorist's direct associates but also indirect

associates, and, therefore provides a more complete picture of those who associate with terrorists and/or are engaged in terrorist activities.

51. Another advantage of the metadata collected in this matter is that it is historical in nature, reflecting contact activity from the past. Given that terrorist operatives often lie dormant for extended periods of time, historical connections are critical to understanding a newly identified target, and metadata may contain links that are unique, pointing to potential targets that may otherwise be missed.

52. Bulk metadata analysis under Section 215 thus enriches NSA intelligence analysts' understanding of the communications tradecraft of terrorist operatives who may be preparing to conduct attacks against the U.S. This analysis can be important considering that terrorist operatives often take affirmative and intentional steps to disguise and obscure their communications.

53. Furthermore, the Section 215 metadata program complements information that the NSA collects via other means and is valuable to NSA, in support of the FBI, for linking possible terrorist-related telephone communications that occur between communicants based solely inside the U.S.

54. As a complementary tool to other intelligence authorities, the NSA's access to telephony metadata improves the likelihood of the Government being able to detect terrorist cell contacts within the U.S. With the metadata collected under Section 215 pursuant to FISC orders, the NSA has the information necessary to perform the call chaining that can enable NSA intelligence analysts to obtain a much fuller understanding of the target and, as a result, allow the NSA to provide FBI with a more complete picture of possible terrorist-related activity occurring inside the U.S.

55. The value of telephony metadata collected under Section 215 is not hypothetical. While many specific instances of the Government's use of telephony metadata under Section 215 remain classified, a number of instances have been disclosed in declassified materials.

56. An illustration of the particular value of the bulk metadata program under Section 215—and a tragic example of what can occur in its absence—is the case of 9/11 hijacker Khalid al-Mihdhar, which I have described above. The Section 215 telephony metadata collection program addresses the information gap that existed at the time of the al-Mihdhar case. It allows the NSA to rapidly and effectively note these types of suspicious contacts and, when appropriate, to tip them to the FBI for follow-on analysis or action.

57. Furthermore, once an identifier has been detected, the NSA can use bulk telephony metadata along with other data sources to quickly identify the larger network and possible co-conspirators both inside and outside the U.S. for further investigation by the FBI with the goal of preventing future terrorist attacks.

58. As the case examples in the FBI declaration accompanying this declaration demonstrate, Section 215 bulk telephony metadata is a resource not only in isolation, but also for investigating threat leads obtained from other SIGINT collection or partner agencies. This is especially true for the NSA-FBI partnership. The Section 215 telephony metadata program enables NSA intelligence analysts to evaluate potential threats that it receives from or reports to the FBI in a more complete manner than if this data source were unavailable.

59. Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while

Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions.

60. Reliance solely on traditional, case-by-case intelligence gathering methods, restricted to known terrorist identifiers, would significantly impair the NSA's ability to accomplish many of the aforementioned objectives.

61. Without the ability to obtain and analyze bulk metadata, the NSA would lose a tool for detecting communication chains that link to identifiers associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts both within the U.S. and abroad. Having the bulk telephony metadata available to query is part of this effort, as there is no way to know in advance which numbers will be responsive to the authorized queries.

62. The bulk metadata allows retrospective analyses of prior communications of newly discovered terrorists in an efficacious manner. Any other means that might be used to attempt to conduct similar analyses would require multiple, time-consuming steps that would frustrate needed rapid analysis in emergent situations, and could fail to capture some data available through bulk metadata analysis.

63. If the telephony metadata are not aggregated and retained for a sufficient period of time, it will not be possible for the NSA to detect chains of communications that cross different providers and telecommunications networks. But for the NSA's metadata collection, the NSA

would need to seek telephonic records from multiple providers whenever a need to inquire arose, and each such provider may not maintain records in a format that is subject to a standardized query.

64. Thus, the Government could not achieve the aforementioned benefits of Section 215 metadata collection through alternative means.

65. The use of more targeted means of collection—whether through subpoenas, national security letters (“NSLs”), or pen-register and trap-and-trace (“PR/TT”) devices authorized under the FISA—solely of records directly pertaining to a terrorism subject would fail to permit the comprehensive and retrospective analyses detailed above of communication chains that might, and sometimes do, reveal previously unknown persons of interest in terrorism investigations. Targeted inquiries also would fail to capture communications chains and overlaps that can be of investigatory significance, because targeted inquiries would eliminate the NSA’s ability to collect and analyze metadata of communications occurring at the second “hop” from a terrorist suspect’s initial “seed”; rather, they would only reveal communications directly involving the specific targets in question. In other words, targeted inquiries would capture only one “hop.” As a result, the Government’s ability to discover and analyze communications metadata revealing the fact that as-yet unknown identifiers are linked in a chain of communications with identified terrorist networks would be impaired.

66. In sum, any order immediately barring the Government from employing the Section 215 metadata collection program would deprive the Government of unique capabilities that could not be completely replicated by other means, and as a result would cause an increased risk to national security and the safety of the American public.

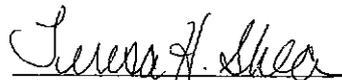
67. Beyond harming national security and the Government's counterterrorism capabilities, plaintiff's proposed preliminary injunction would seriously burden the Government. While plaintiff seeks an order barring the Government from collecting metadata reflecting her calls, the Government does not know plaintiff's phone number(s), and would need plaintiff to identify all numbers that she uses to even attempt to implement such an injunction. Ironically, as explained above, these numbers will not be available to NSA analysts unless they are within two hops of a call chain of a number that, based on RAS, is associated with a foreign terrorist organization.

[Remainder of page intentionally left blank]

68. Even if plaintiff's phone numbers were available, extraordinarily burdensome technical and logistical hurdles to compliance with a preliminary injunction order would remain. Technical experts would have to develop a solution such as removing the plaintiff's numbers from the system upon receipt of each batch of metadata or developing a capability whereby plaintiff's numbers would be received by NSA but would not be visible in response to an authorized query. To identify, design, build, and test the best implementation solution would potentially require the creation of new full-time positions and could take six months or more to implement. Once implemented, any potential solution could undermine the results of any authorized query of a phone number that, based on RAS, is associated with one of the identified foreign terrorist organizations by eliminating, or cutting off potential call chains. If this Court were to grant a preliminary injunction and the defendants were to later prevail on the merits of this litigation, it could prove extremely difficult to develop a solution to restore any removed records and would likely take considerable resources and several months to build, test, and implement a capability suited to this task.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

DATE: 1-23-14



Teresa H. Shea
Signals Intelligence Director
National Security Agency

~~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 13-109

AMENDED MEMORANDUM OPINION

I. Background.

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~~

~~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.

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

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

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.

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

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

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.

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

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

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.

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

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

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.'"

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

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

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).

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

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

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).

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

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

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

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

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

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.

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

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

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.

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

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

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).

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

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

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.

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

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

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

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

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

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.

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

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

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

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

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

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.

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

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

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

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

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

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.

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

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

[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]

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

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

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]nalytists 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~~

~~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~~

~~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,

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

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

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.

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

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

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.*

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

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

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)).

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

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

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.*

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

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

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

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

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

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.

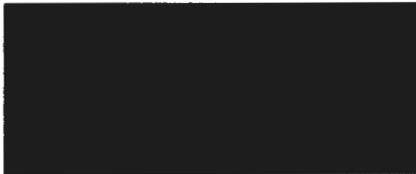
For these reasons, for the reasons stated in the Primary Order appended hereto, and pursuant to 50 U.S.C. § 1861(c)(1), the Court has GRANTED the Orders requested by the government.

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~~

~~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 13-109

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~~

~~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.

⁴ [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 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~~

~~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

~~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]

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~~

~~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}

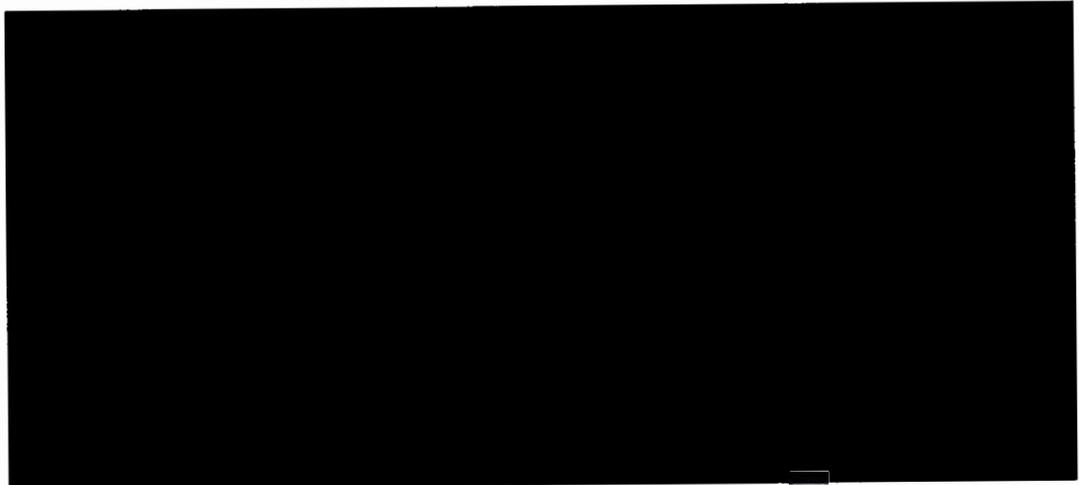
⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, 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]

~~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:

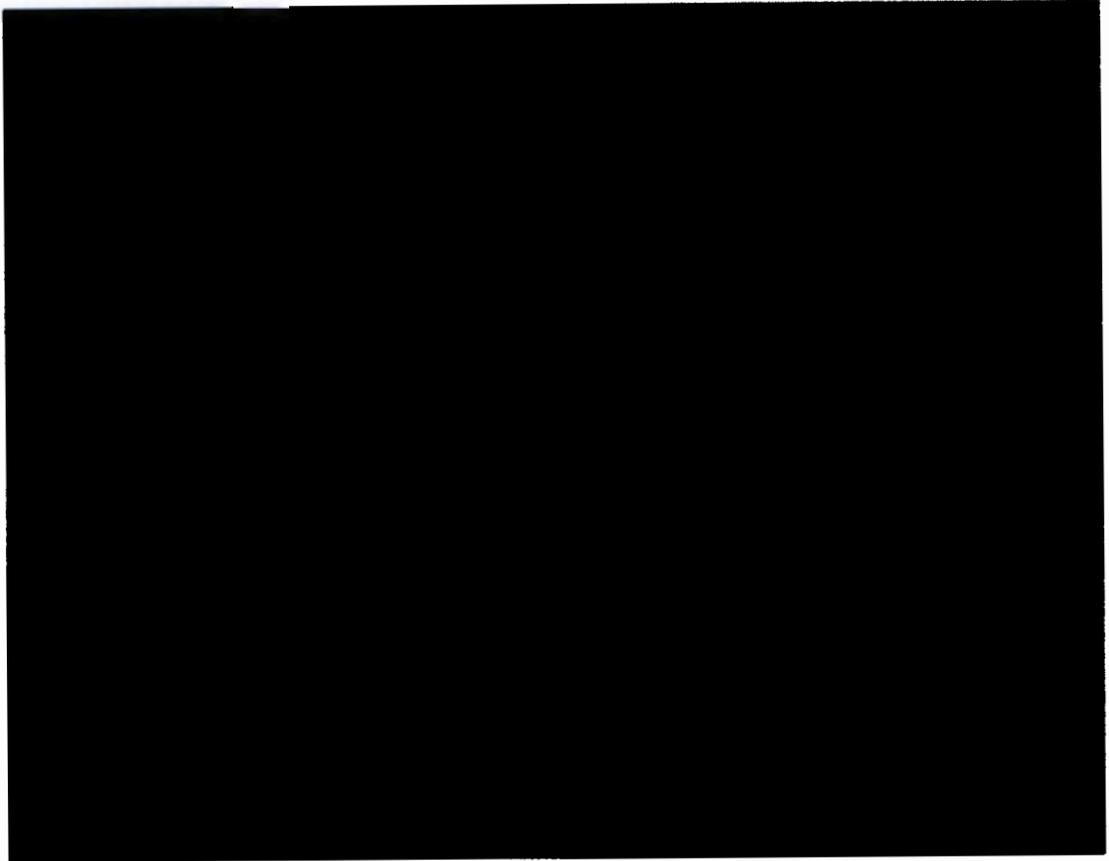


¹¹ This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

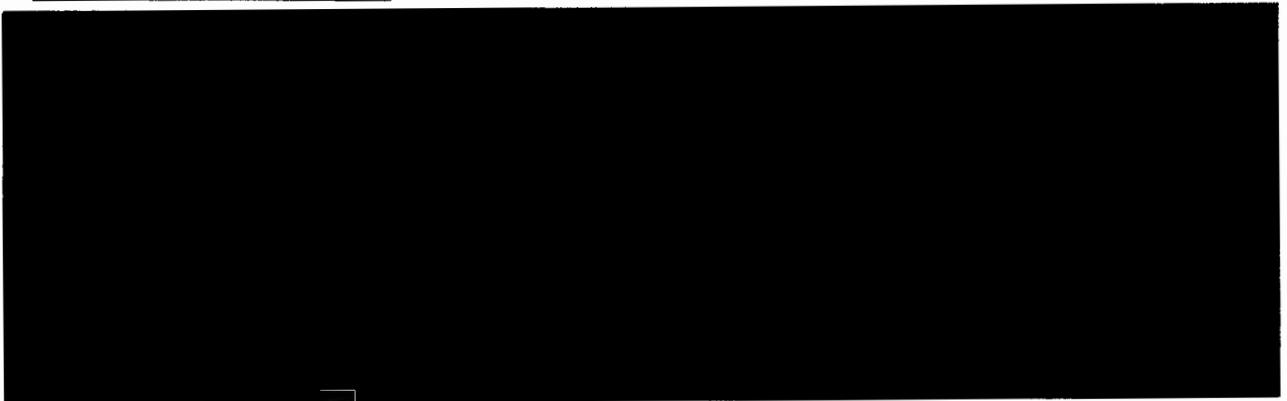
¹² As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms 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~~

~~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~~

~~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) 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~~

~~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

10-9-13 10:45

Claire V. Eagan

CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

[REDACTED]

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

~~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 13-158

MEMORANDUM

The Court has today issued the Primary Order appended hereto granting the "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" ("Application"), which was submitted to the Court on October

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

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

10, 2013, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk.

The Primary Order appended hereto renews the production of records made pursuant to the similar Primary Order issued by the Honorable Claire V. Eagan of this Court on July 19, 2013 in Docket Number BR 13-109 ("July 19 Primary Order"). On August 29, 2013, Judge Eagan issued an Amended Memorandum Opinion setting forth her reasons for issuing the July 19 Primary Order ("August 29 Opinion"). Following a declassification review by the Executive Branch, the Court published the July 19 Primary Order and August 29 Opinion in redacted form on September 17, 2013.

The call detail records to be produced pursuant to the orders issued today in the above-captioned docket are identical in scope and nature to the records produced in response to the orders issued by Judge Eagan in Docket Number BR 13-109. The records will be produced on terms identical to those set out in Judge Eagan's July 19 Primary Order and for the same purpose, and the information acquired by NSA through the production will be subject to the same provisions for oversight and identical restrictions on access, retention, and dissemination.

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

Page 2

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

This is the first time that the undersigned has entertained an application requesting the bulk production of call detail records. The Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application. The Court writes separately to discuss briefly the issues of "relevance" and the inapplicability of the Fourth Amendment to the production.

Although the definition of relevance set forth in Judge Eagan's decision is broad, the Court is persuaded that that definition is supported by the statutory analysis set out in the August 29 Opinion. That analysis is reinforced by Congress's re-enactment of Section 215 after receiving information about the government's and the FISA Court's interpretation of the statute. Although the existence of this program was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215. Accordingly, the re-enactment of Section 215 without change in 2011 triggered the doctrine of ratification through re-enactment, which provides a strong reason for this Court to continue to adhere to its prior interpretation of Section 215. See Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also EEOC v. Shell Oil Co., 466 U.S. 54, 69 (1984); Haig v. Agee, 453 U.S. 280, 297-98 (1981).

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

Page 3

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

The undersigned also agrees with Judge Eagan that, under Smith v. Maryland, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. In Smith, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search for purposes of the Fourth Amendment. In so holding, the Court stressed that the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls.

The Supreme Court's more recent decision in United States v. Jones, — U.S. —, 132 S. Ct. 945 (2012), does not point to a different result here. Jones involved the acquisition of a different type of information through different means. There, law enforcement officers surreptitiously attached a Global Positioning System (GPS) device to the defendant's vehicle and used it to track his location for 28 days. The Court held in Justice Scalia's majority opinion that the officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, a constitutionally-protected area. The majority declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy.

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

Page 4

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

Five Justices in Jones signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection even without any physical intrusion. This matter, however, involves no such monitoring. Like Smith, this case concerns the acquisition of non-content metadata other than location information. See Aug. 29 Op. at 29 at 4 n.5; id. at 6 & n.10.

Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital age." See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith and United States v. Miller, 425 U.S. 435, 443 (1976), as examples of decisions relying upon that premise). But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones. See id. ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."). The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony

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

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

metadata such as the information to be produced in this matter.

In light of the public interest in this matter and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion and July 19 Primary Order, the undersigned requests pursuant to FISC Rule 62 that this Memorandum and the accompanying Primary Order also be published and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 11th day of October, 2013.

Mary A. McLaughlin
MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court



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

~~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 - 158

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 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

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

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

Accordingly, and as further explained in the accompanying Memorandum, 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~~

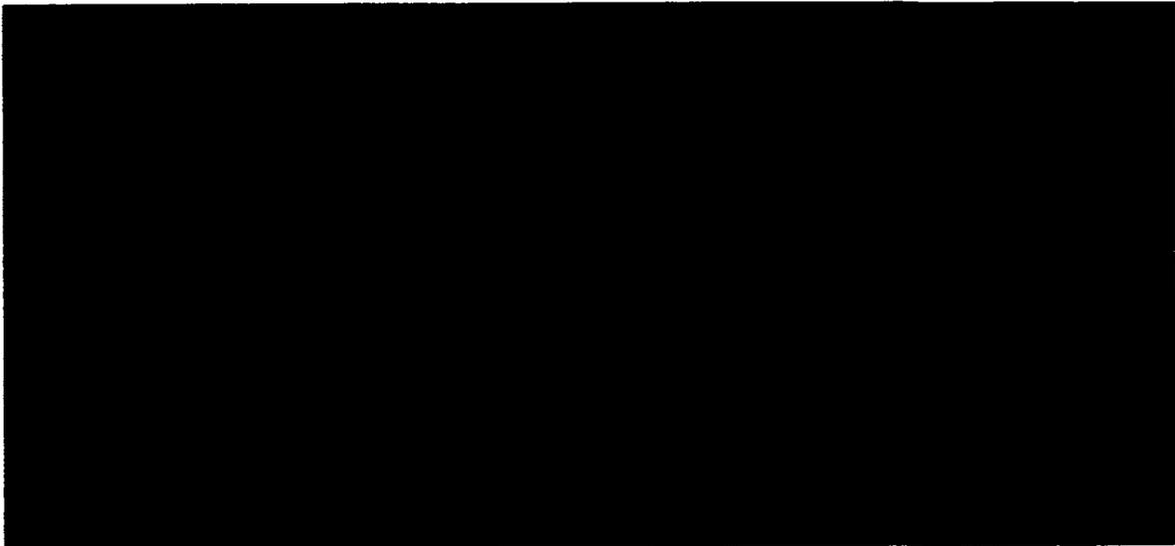
~~TOP SECRET//SI//NOFORN~~

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.



~~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 queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration of [REDACTED] [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,

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~~

through 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]

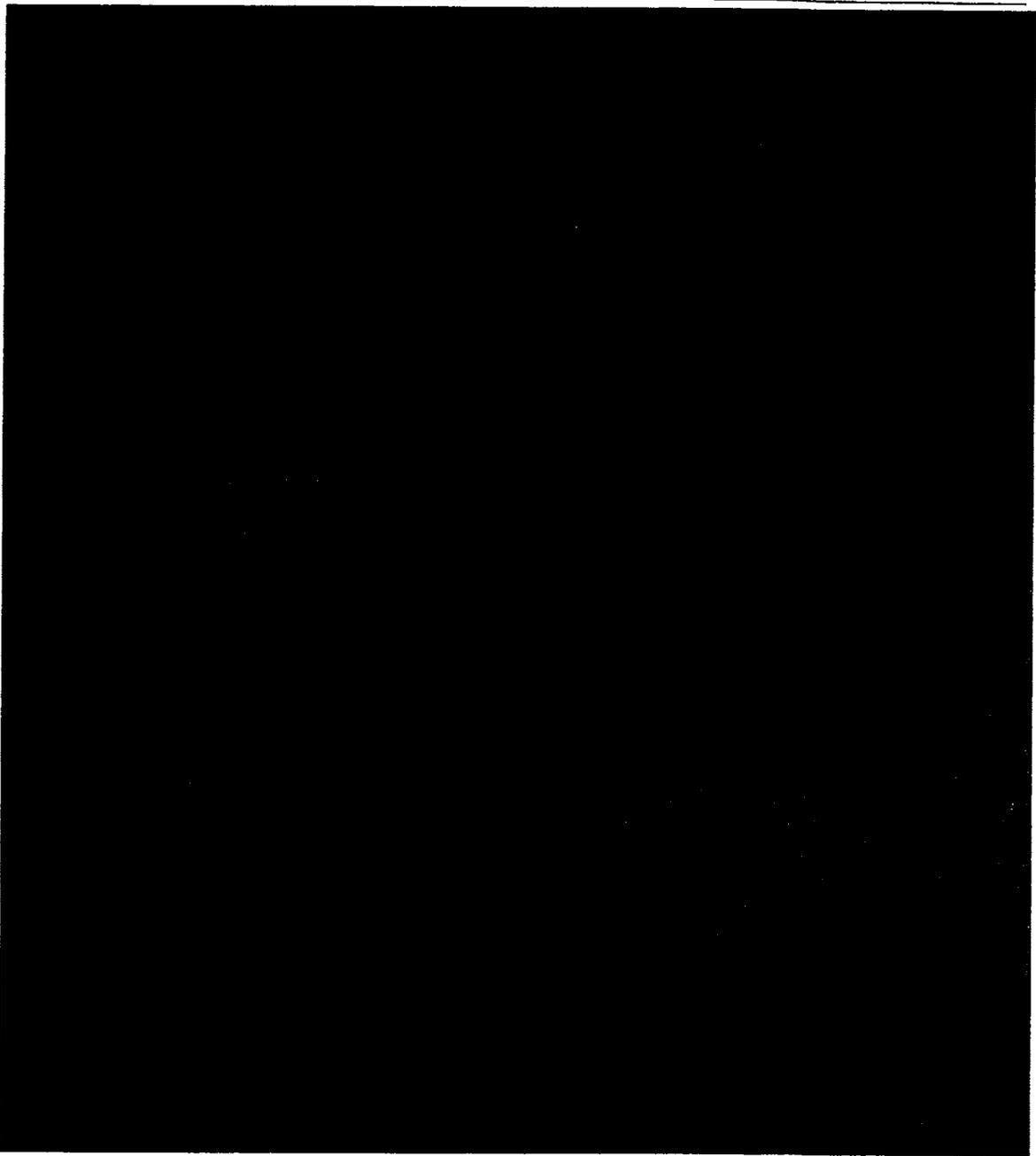
⁶ This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[REDACTED]

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

~~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] 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~~

~~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}

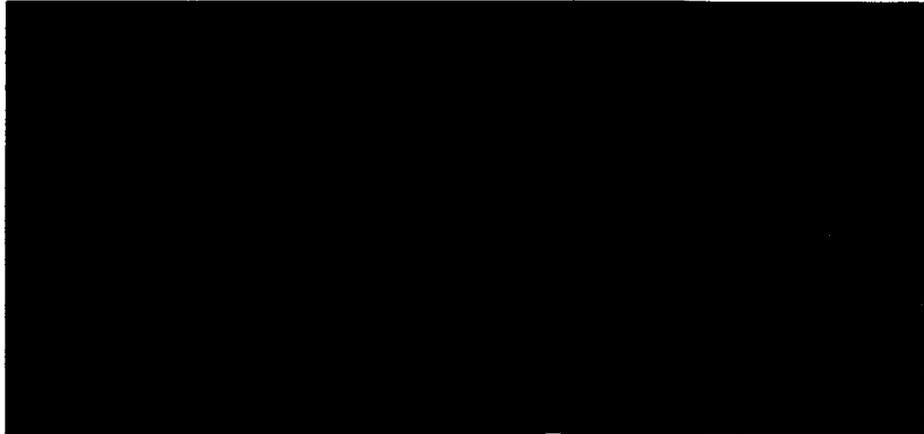
⁹ The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, 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.

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]

~~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:

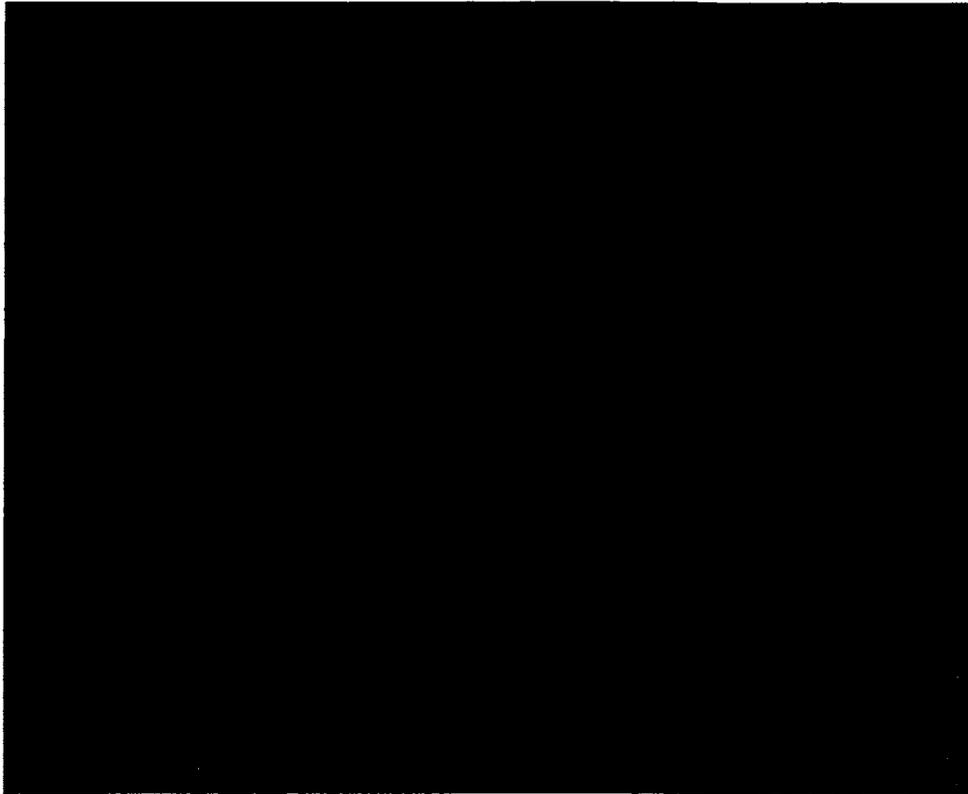


¹¹ This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

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~~

~~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~~

~~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) 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.

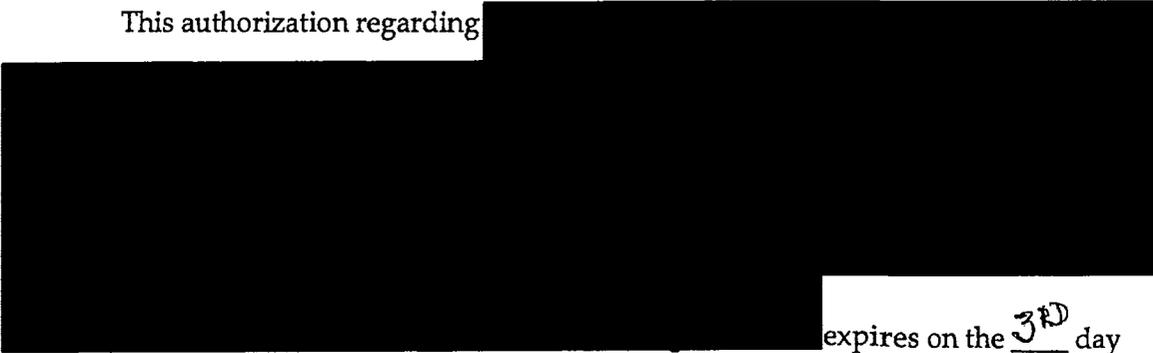
Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials

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

~~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



expires on the 3RD day

of January, 2014, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time

10-11-2013 P12:05

Mary A. McLaughlin

MARY A. MCLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

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



Get Email Updates Contact Us

Home • Briefing Room • Speeches & Remarks

Search WhiteHouse.gov Search

The White House

Office of the Press Secretary

For Immediate Release

January 17, 2014

Remarks by the President on Review of Signals Intelligence

Department of Justice
Washington, D.C.

11:15 A.M. EST

THE PRESIDENT: At the dawn of our Republic, a small, secret surveillance committee borne out of the "The Sons of Liberty" was established in Boston. And the group's members included Paul Revere. At night, they would patrol the streets, reporting back any signs that the British were preparing raids against America's early Patriots.

Throughout American history, intelligence has helped secure our country and our freedoms. In the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of campfires. In World War II, code-breakers gave us insights into Japanese war plans, and when Patton marched across Europe, intercepted communications helped save the lives of his troops. After the war, the rise of the Iron Curtain and nuclear weapons only increased the need for sustained intelligence gathering. And so, in the early days of the Cold War, President Truman created the National Security Agency, or NSA, to give us insights into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe.

Throughout this evolution, we benefited from both our Constitution and our traditions of limited government. U.S. intelligence agencies were anchored in a system of checks and balances -- with oversight from elected leaders, and protections for ordinary citizens. Meanwhile, totalitarian states like East Germany offered a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes.

In fact, even the United States proved not to be immune to the abuse of surveillance. And in the 1960s, government spied on civil rights leaders and critics of the Vietnam War. And partly in response to these revelations, additional laws were established in the 1970s to ensure that our intelligence capabilities could not be misused against our citizens. In the long, twilight struggle against Communism, we had been reminded that the very liberties that we sought to preserve could not be sacrificed at the altar of national security.

If the fall of the Soviet Union left America without a competing superpower, emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. Moreover, these new threats raised new legal and new policy questions. For while few doubted the legitimacy of spying on hostile states, our framework of laws was not fully adapted to prevent terrorist attacks by individuals acting on their own, or acting in small, ideologically driven groups on behalf of a foreign power.

The horror of September 11th brought all these issues to the fore. Across the political spectrum, Americans recognized that we had to adapt to a world in which a bomb could be built in a basement, and our electric grid could be shut down by operators an ocean away. We were shaken by the signs we had missed leading up to the attacks -- how the hijackers had made phone calls to known extremists and traveled to suspicious places. So we demanded that our intelligence



LATEST BLOG POSTS

January 17, 2014 1:20 PM EST

Celebrating Benjamin Franklin's Birthday on Founders Online

In honor of Benjamin Franklin's birthday, the National Archives is celebrating by adding the annotated volumes from The Papers of Benjamin Franklin to Founders Online .

January 17, 2014 12:30 PM EST

Taking Action to Expand College Opportunity

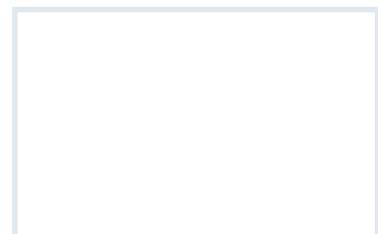
A group of leaders in higher education join the President and First Lady at the White House to take the next step toward ensuring that every child, rich or poor, has the opportunity for a quality college education so they can get ahead.

January 17, 2014 12:00 PM EST

Survey: Electronic Health Records Incentive Program Is on Track

The adoption of electronic health records is reflected today in a release from the Centers for Disease Control and Prevention's National Center for Health Statistics which provides a view of the Medicare and Medicaid EHR Incentive Program and indicates the program is healthy and growing steadily.

VIEW ALL RELATED BLOG POSTS ►



community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack.

It is hard to overstate the transformation America's intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers. Instead, they were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.

And it is a testimony to the hard work and dedication of the men and women of our intelligence community that over the past decade we've made enormous strides in fulfilling this mission. Today, new capabilities allow intelligence agencies to track who a terrorist is in contact with, and follow the trail of his travel or his funding. New laws allow information to be collected and shared more quickly and effectively between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives -- not just here in the United States, but around the globe.

And yet, in our rush to respond to a very real and novel set of threats, the risk of government overreach -- the possibility that we lose some of our core liberties in pursuit of security -- also became more pronounced. We saw, in the immediate aftermath of 9/11, our government engaged in enhanced interrogation techniques that contradicted our values. As a Senator, I was critical of several practices, such as warrantless wiretaps. And all too often new authorities were instituted without adequate public debate.

Through a combination of action by the courts, increased congressional oversight, and adjustments by the previous administration, some of the worst excesses that emerged after 9/11 were curbed by the time I took office. But a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties.

First, the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach. And at a time when more and more of our lives are digital, that prospect is disquieting for all of us.

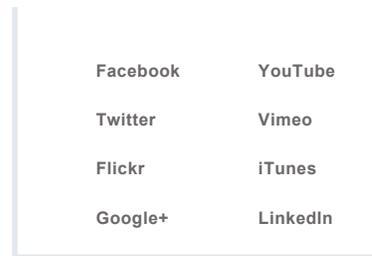
Second, the combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. It's a powerful tool. But the government collection and storage of such bulk data also creates a potential for abuse.

Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And the whole point of intelligence is to obtain information that is not publicly available. But America's capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

And finally, intelligence agencies cannot function without secrecy, which makes their work less subject to public debate. Yet there is an inevitable bias not only within the intelligence community, but among all of us who are responsible for national security, to collect more information about the world, not less. So in the absence of institutional requirements for regular debate -- and oversight that is public, as well as private or classified -- the danger of government overreach becomes more acute. And this is particularly true when surveillance technology and our reliance on digital information is evolving much faster than our laws.

For all these reasons, I maintained a healthy skepticism toward our surveillance programs after I became President. I ordered that our programs be reviewed by my national security team and our lawyers, and in some cases I ordered changes in how we did business. We increased oversight and auditing, including new structures aimed at compliance. Improved rules were proposed by the government and approved by the Foreign Intelligence Surveillance Court. And we sought to keep Congress continually updated on these activities.

What I did not do is stop these programs wholesale -- not only because I felt that they made us more secure, but also because nothing in that initial review, and nothing that I have learned since,



indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens.

To the contrary, in an extraordinarily difficult job -- one in which actions are second-guessed, success is unreported, and failure can be catastrophic -- the men and women of the intelligence community, including the NSA, consistently follow protocols designed to protect the privacy of ordinary people. They're not abusing authorities in order to listen to your private phone calls or read your emails. When mistakes are made -- which is inevitable in any large and complicated human enterprise -- they correct those mistakes. Laboring in obscurity, often unable to discuss their work even with family and friends, the men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots. What sustains those who work at NSA and our other intelligence agencies through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation.

Now, to say that our intelligence community follows the law, and is staffed by patriots, is not to suggest that I or others in my administration felt complacent about the potential impact of these programs. Those of us who hold office in America have a responsibility to our Constitution, and while I was confident in the integrity of those who lead our intelligence community, it was clear to me in observing our intelligence operations on a regular basis that changes in our technological capabilities were raising new questions about the privacy safeguards currently in place.

Moreover, after an extended review of our use of drones in the fight against terrorist networks, I believed a fresh examination of our surveillance programs was a necessary next step in our effort to get off the open-ended war footing that we've maintained since 9/11. And for these reasons, I indicated in a speech at the National Defense University last May that we needed a more robust public discussion about the balance between security and liberty. Of course, what I did not know at the time is that within weeks of my speech, an avalanche of unauthorized disclosures would spark controversies at home and abroad that have continued to this day.

And given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or his motivations; I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come.

Regardless of how we got here, though, the task before us now is greater than simply repairing the damage done to our operations or preventing more disclosures from taking place in the future. Instead, we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. They are going to continue to be a major problem. And for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.

This effort will not be completed overnight, and given the pace of technological change, we shouldn't expect this to be the last time America has this debate. But I want the American people to know that the work has begun. Over the last six months, I created an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform. I consulted with the Privacy and Civil Liberties Oversight Board, created by Congress. I've listened to foreign partners, privacy advocates, and industry leaders. My administration has spent countless hours considering how to approach intelligence in this era of diffuse threats and technological revolution. So before outlining specific changes that I've ordered, let me make a few broad observations that have emerged from this process.

First, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats, and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications -- whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to

ensure that hackers do not empty your bank accounts. We are expected to protect the American people; that requires us to have capabilities in this field.

Moreover, we cannot unilaterally disarm our intelligence agencies. There is a reason why BlackBerrys and iPhones are not allowed in the White House Situation Room. We know that the intelligence services of other countries -- including some who feign surprise over the Snowden disclosures -- are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems. We know that.

Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people.

Second, just as ardent civil libertarians recognize the need for robust intelligence capabilities, those with responsibilities for our national security readily acknowledge the potential for abuse as intelligence capabilities advance and more and more private information is digitized. After all, the folks at NSA and other intelligence agencies are our neighbors. They're our friends and family. They've got electronic bank and medical records like everybody else. They have kids on Facebook and Instagram, and they know, more than most of us, the vulnerabilities to privacy that exist in a world where transactions are recorded, and emails and text and messages are stored, and even our movements can increasingly be tracked through the GPS on our phones.

Third, there was a recognition by all who participated in these reviews that the challenges to our privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer and your smartphone periodically. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power.

I make these observations to underscore that the basic values of most Americans when it comes to questions of surveillance and privacy converge a lot more than the crude characterizations that have emerged over the last several months. Those who are troubled by our existing programs are not interested in repeating the tragedy of 9/11, and those who defend these programs are not dismissive of civil liberties.

The challenge is getting the details right, and that is not simple. In fact, during the course of our review, I have often reminded myself I would not be where I am today were it not for the courage of dissidents like Dr. King, who were spied upon by their own government. And as President, a President who looks at intelligence every morning, I also can't help but be reminded that America must be vigilant in the face of threats.

Fortunately, by focusing on facts and specifics rather than speculation and hypotheticals, this review process has given me -- and hopefully the American people -- some clear direction for change. And today, I can announce a series of concrete and substantial reforms that my administration intends to adopt administratively or will seek to codify with Congress.

First, I have approved a new presidential directive for our signals intelligence activities both at home and abroad. This guidance will strengthen executive branch oversight of our intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of American companies; and our commitment to privacy and basic liberties. And we will review decisions about intelligence priorities and sensitive targets on an annual basis so that our actions are regularly scrutinized by my senior national security team.

Second, we will reform programs and procedures in place to provide greater transparency to our surveillance activities, and fortify the safeguards that protect the privacy of U.S. persons. Since we began this review, including information being released today, we have declassified over 40 opinions and orders of the Foreign Intelligence Surveillance Court, which provides judicial review of

some of our most sensitive intelligence activities -- including the Section 702 program targeting foreign individuals overseas, and the Section 215 telephone metadata program.

And going forward, I'm directing the Director of National Intelligence, in consultation with the Attorney General, to annually review for the purposes of declassification any future opinions of the court with broad privacy implications, and to report to me and to Congress on these efforts. To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.

Third, we will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security. Specifically, I am asking the Attorney General and DNI to institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702.

Fourth, in investigating threats, the FBI also relies on what's called national security letters, which can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation. These are cases in which it's important that the subject of the investigation, such as a possible terrorist or spy, isn't tipped off. But we can and should be more transparent in how government uses this authority.

I have therefore directed the Attorney General to amend how we use national security letters so that this secrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

This brings me to the program that has generated the most controversy these past few months -- the bulk collection of telephone records under Section 215. Let me repeat what I said when this story first broke: This program does not involve the content of phone calls, or the names of people making calls. Instead, it provides a record of phone numbers and the times and lengths of calls -- metadata that can be queried if and when we have a reasonable suspicion that a particular number is linked to a terrorist organization.

Why is this necessary? The program grew out of a desire to address a gap identified after 9/11. One of the 9/11 hijackers -- Khalid al-Mihdhar -- made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. And this capability could also prove valuable in a crisis. For example, if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence. Being able to quickly review phone connections to assess whether a network exists is critical to that effort.

In sum, the program does not involve the NSA examining the phone records of ordinary Americans. Rather, it consolidates these records into a database that the government can query if it has a specific lead -- a consolidation of phone records that the companies already retained for business purposes. The review group turned up no indication that this database has been intentionally abused. And I believe it is important that the capability that this program is designed to meet is preserved.

Having said that, I believe critics are right to point out that without proper safeguards, this type of program could be used to yield more information about our private lives, and open the door to more intrusive bulk collection programs in the future. They're also right to point out that although the telephone bulk collection program was subject to oversight by the Foreign Intelligence Surveillance Court and has been reauthorized repeatedly by Congress, it has never been subject to vigorous public debate.

For all these reasons, I believe we need a new approach. I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.

This will not be simple. The review group recommended that our current approach be replaced by one in which the providers or a third party retain the bulk records, with government accessing information as needed. Both of these options pose difficult problems. Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new privacy concerns. On the other hand, any third party maintaining a single, consolidated database would be carrying out what is essentially a government function but with more expense, more legal ambiguity, potentially less accountability -- all of which would have a doubtful impact on increasing public confidence that their privacy is being protected.

During the review process, some suggested that we may also be able to preserve the capabilities we need through a combination of existing authorities, better information sharing, and recent technological advances. But more work needs to be done to determine exactly how this system might work.

Because of the challenges involved, I've ordered that the transition away from the existing program will proceed in two steps. Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three. And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency.

Next, step two, I have instructed the intelligence community and the Attorney General to use this transition period to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself. They will report back to me with options for alternative approaches before the program comes up for reauthorization on March 28th. And during this period, I will consult with the relevant committees in Congress to seek their views, and then seek congressional authorization for the new program as needed.

Now, the reforms I'm proposing today should give the American people greater confidence that their rights are being protected, even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe. And I recognize that there are additional issues that require further debate. For example, some who participated in our review, as well as some members of Congress, would like to see more sweeping reforms to the use of national security letters so that we have to go to a judge each time before issuing these requests. Here, I have concerns that we should not set a standard for terrorism investigations that is higher than those involved in investigating an ordinary crime. But I agree that greater oversight on the use of these letters may be appropriate, and I'm prepared to work with Congress on this issue.

There are also those who would like to see different changes to the FISA Court than the ones I've proposed. On all these issues, I am open to working with Congress to ensure that we build a broad consensus for how to move forward, and I'm confident that we can shape an approach that meets our security needs while upholding the civil liberties of every American.

Let me now turn to the separate set of concerns that have been raised overseas, and focus on America's approach to intelligence collection abroad. As I've indicated, the United States has unique responsibilities when it comes to intelligence collection. Our capabilities help protect not only our nation, but our friends and our allies, as well. But our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy, too. And the leaders of our close friends and allies deserve to know that if I want to know what they think about an issue, I'll pick up the phone and call them, rather than turning to surveillance. In other words, just as we balance security and privacy at home, our global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and leaders around the world.

For that reason, the new presidential directive that I've issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance. To begin with, the directive makes clear that the United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary folks. I've also made it clear that the United States does not collect intelligence to suppress criticism or dissent, nor do we collect intelligence to disadvantage people on the basis of their ethnicity, or race, or gender, or sexual orientation, or religious beliefs. We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors.

And in terms of our bulk collection of signals intelligence, U.S. intelligence agencies will only use such data to meet specific security requirements: counterintelligence, counterterrorism, counter-proliferation, cybersecurity, force protection for our troops and our allies, and combating transnational crime, including sanctions evasion.

In this directive, I have taken the unprecedented step of extending certain protections that we have for the American people to people overseas. I've directed the DNI, in consultation with the Attorney General, to develop these safeguards, which will limit the duration that we can hold personal information, while also restricting the use of this information.

The bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account in our policies and procedures. This applies to foreign leaders as well. Given the understandable attention that this issue has received, I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies. And I've instructed my national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.

Now let me be clear: Our intelligence agencies will continue to gather information about the intentions of governments -- as opposed to ordinary citizens -- around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective. But heads of state and government with whom we work closely, and on whose cooperation we depend, should feel confident that we are treating them as real partners. And the changes I've ordered do just that.

Finally, to make sure that we follow through on all these reforms, I am making some important changes to how our government is organized. The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. We will appoint a senior official at the White House to implement the new privacy safeguards that I have announced today. I will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism.

I have also asked my counselor, John Podesta, to lead a comprehensive review of big data and privacy. And this group will consist of government officials who, along with the President's Council of Advisors on Science and Technology, will reach out to privacy experts, technologists and business leaders, and look how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.

For ultimately, what's at stake in this debate goes far beyond a few months of headlines, or passing tensions in our foreign policy. When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed. Whether it's the ability of individuals to communicate ideas; to access information that would have once filled every great library in every country in the world; or to forge bonds with people on other sides of the globe, technology is remaking what is possible for individuals, and for institutions, and for the international order. So while the reforms that I have announced will point us in a new direction, I am mindful that more work will be needed in the future.

One thing I'm certain of: This debate will make us stronger. And I also know that in this time of change, the United States of America will have to lead. It may seem sometimes that America is being held to a different standard. And I'll admit the readiness of some to assume the worst motives by our government can be frustrating. No one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account. But let's remember: We are held to a different standard precisely because we have been at the forefront of defending personal privacy and human dignity.

As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control. Having faced down the dangers of totalitarianism and fascism and communism, the world expects us to stand up for the

principle that every person has the right to think and write and form relationships freely -- because individual freedom is the wellspring of human progress.

Those values make us who we are. And because of the strength of our own democracy, we should not shy away from high expectations. For more than two centuries, our Constitution has weathered every type of change because we have been willing to defend it, and because we have been willing to question the actions that have been taken in its defense. Today is no different. I believe we can meet high expectations. Together, let us chart a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for.

Thank you. God bless you. May God bless the United States of America. (Applause.)

END
11:57 A.M. EST

WWW.WHITEHOUSE.GOV
En español | Accessibility | Copyright Information | Privacy Policy | Contact
USA.gov | Developers | Apply for a Job

~~TOP SECRET//COMINT//NOFORN~~

~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- ~~(TS//SI//NF)~~ Provisions of the USA PATRIOT Act affected by reauthorization legislation support two sensitive intelligence collection programs;
- ~~(TS//SI//NF)~~ These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by anyone in the government, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the Foreign Intelligence Surveillance Court ("FISA Court") and Congress;
- ~~(TS//SI//NF)~~ The Executive Branch, including DOJ, ODNI, and NSA, takes any compliance problems in the programs very seriously, and substantial progress has been made in addressing those problems.  and
- ~~(TS//SI//NF)~~ NSA's bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Classified by: Assistant Attorney General, NSD
Reason: 1.4(c)
Declassify on: 11 December 2034~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the National Security Agency (NSA) intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al-Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ Today, under Foreign Intelligence Surveillance Court authorization pursuant to the "business records" authority of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorism target overseas. This and similar programs operated pursuant to FISA provide valuable intelligence information.

(U) USA PATRIOT Act reauthorization legislation currently pending in both the House and the Senate would alter, among other things, language in two parts of FISA: Section 215 and the FISA "pen register/trap and trace" (or "pcn-trap") authority. Absent legislation, Section 215 will expire on December 31, 2009, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The FISA pen-trap authority does not expire, but the pending legislation in the Senate and House includes amendments of this provision.

~~(TS//SI//NF)~~ The Section 215 and pen-trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant uses of these authorities are to support two critical and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from telecommunications providers [REDACTED]

[REDACTED] Although these programs have been briefed to

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The 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.

~~(TS//SI//NF)~~ Under the program based on the pen-trap provisions in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail and the time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment. [REDACTED]

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~Checks and BalancesFISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen-trap provision. Before obtaining any information from a telecommunication service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before an NSA analyst may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [REDACTED]

The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. There are also limits on how long the collected data can be retained (5 years in the Section 215 program, and 4½ years in the pen-trap program).

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, to include hearings, briefings, and, with respect to the Intelligence Committees, visits to NSA. In addition, the Intelligence Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ There have been a number of technical compliance problems and human implementation errors in these two bulk collection programs, discovered as a result of Department of Justice reviews and internal NSA oversight. However, neither the Department, NSA nor the FISA Court has found any intentional or bad-faith violations. The problems generally involved the implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the Court's orders. In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered "end-to-end" reviews of the Section 215 and pen-trap collection programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection. In early September of 2009, the Director of NSA made a presentation to the FISA Court about the steps taken to address the compliance issues. All

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify the network of contacts that a targeted number or address is connected to, whenever there is RAS that the number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata. (Communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content.). The more metadata NSA has access to, the more likely it is that NSA can identify or discover the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen-trap bulk collection programs provide a vital capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~~~(TS//SI//NF)~~ **Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization**

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- (U) Section 215 of the USA PATRIOT Act, which expires at the end of February 2011, allows the government, upon approval of the Foreign Intelligence Surveillance Court ("FISA Court"), to obtain access to certain business records for national security investigations;
- (U) Section 402 of the Foreign Intelligence Surveillance Act ("FISA"), which is not subject to a sunset, allows the government, upon approval of the FISA Court, to install and use a pen register or trap and trace ("pen/trap") device for national security investigations;
- ~~(TS//SI//NF)~~ These authorities support two sensitive and important intelligence collection programs. These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect 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;
- ~~(TS//SI//NF)~~ 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;
- ~~(TS//SI//NF)~~ Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court; and
- ~~(TS//SI//NF)~~ The National Security Agency's (NSA) bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Derived From: NSA/CSSM 1-52
Date: 20070108
Declassify On: 20360101~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the NSA intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."

~~(TS//SI//NF)~~ 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 that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorist overseas. This and similar programs operated pursuant to FISA, including exercise of pen/trap authorities, provide valuable intelligence information.

(U) Absent legislation, Section 215 will expire on February 28, 2011, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The pen/trap authority does not expire.

~~(TS//SI//NF)~~ The Section 215 and pen/trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant use of these authorities is to support two important and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States. [REDACTED]

[REDACTED] Although these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from certain telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The 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.

~~(TS//SI//NF)~~ Under the program based on the pen/trap provision in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail, certain routing information, and the date and time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment.

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

[REDACTED]

However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.

Checks and Balances

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen/trap provision. Before obtaining any information from a telecommunications service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed “minimization procedures” required by the FISA Court that govern the retention and dissemination of the information obtained. Before NSA analysts may query bulk records, they must have reasonable articulable suspicion – referred to as “RAS” – that the number or e-mail address they submit is associated with [REDACTED]

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

[REDACTED] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. The bulk data collected under each program can be retained for 5 years.

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, through hearings, briefings, and visits to NSA. In addition, the Intelligence and Judiciary Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ In 2009, a number of technical compliance problems and human implementation errors in these two bulk collection programs were discovered as a result of Department of Justice (DOJ) reviews and internal NSA oversight. However, neither DOJ, NSA, nor the FISA Court has found any intentional or bad-faith violations. [REDACTED]

[REDACTED]

In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The FISA Court placed several restrictions on aspects of the business records collection program until the compliance processes were improved to its satisfaction. [REDACTED]

[REDACTED]

(U) The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed safeguards that, together with greater efforts by the Executive Branch, have resulted in significant and effective changes in the compliance program.

(U) All parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community’s early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States that may be contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and entirely domestic connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify and assess the network of contacts that a targeted number or address is connected to, whenever there is RAS that the targeted number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata – but always based on links to a number or e-mail address which itself is associated with a counterterrorism target. (Again, communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content) The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses. Information discovered through NSA’s analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen/trap bulk collection programs provide an important capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

~~TOP SECRET//COMINT//NOFORN~~

~~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 VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13 - 8 0

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon") satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

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

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

Declassified and Approved for Release by DNI
on 07-11-2013 pursuant to E.O. 13526

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

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" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. 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.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

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

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

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

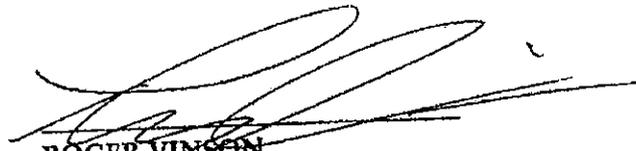
-- Remainder of page intentionally left blank. --

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

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

This authorization requiring the production of certain call detail records or "telephony metadata" created by Verizon expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed _____ Eastern Time
Date Time
 04-25-2013 10:26


ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original. *BQ*

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