

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

<b>Cases</b>	<b>Page</b>
<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.”).<sup>1</sup>

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”).<sup>2</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> [http://www.dni.gov/files/documents/0627/BR%2014-96\\_Primary\\_Order.pdf](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.<sup>3</sup> Most recently, the Foreign Intelligence Surveillance Court reauthorized the Section 215 telephony-

---

<sup>3</sup> 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](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.<sup>4</sup>

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

---

<sup>4</sup> 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.<sup>5</sup> 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

---

<sup>5</sup> 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](http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf).

Primary Order 7-8, 11-12.<sup>6</sup> 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

---

<sup>6</sup> 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).<sup>7</sup>

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

---

<sup>7</sup> [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).<sup>8</sup> 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

---

<sup>8</sup> 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.<sup>9</sup> 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

---

<sup>9</sup> 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.”);<sup>10</sup> *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-96 (FISC June 19, 2014);<sup>11</sup> *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.*

---

<sup>10</sup> This opinion and order are available at: [http://www.dni.gov/files/documents/BR%2014-01\\_FISC\\_Opinion\\_and\\_Order\\_March\\_20\\_2014.pdf](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.

<sup>11</sup> This opinion is available at: [http://www.dni.gov/files/documents/0627/Memorandum\\_Opinion\\_in%20BR\\_14-96.pdf](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).<sup>12</sup> Both the statutory scheme under the Foreign

---

<sup>12</sup> 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.<sup>13</sup> Advances in

---

<sup>13</sup> 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.<sup>14</sup>

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

---

<sup>14</sup> 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.<sup>15</sup> 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

---

<sup>15</sup> 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