[NOT YET SCHEDULED FOR ORAL ARGUMENT]

No. 14-5004, 14-5005, 14-5016, 14-5017

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

LARRY ELLIOTT KLAYMAN et al.,

Appellees/Cross-Appellants,

v.

BARACK HUSSEIN OBAMA et al.,

Appellants/Cross-Appellees.

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

GOVERNMENT APPELLANTS' OPENING BRIEF

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN JR.
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

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), the undersigned counsel certifies as follows:

A. Parties and Amici

These consolidated appeals arise from two related district court cases, No. 13cv851, and No. 13cv881.

No. 14-5004 and its cross-appeal, No. 14-5016, are appeals from the district court's order in No. 13cv851. In those appeals, plaintiffs-appellees (and cross-appellants) are Larry Elliot Klayman, Charles Strange, and Mary Ann Strange. Defendants-appellants (and cross-appellees) include Barack Hussein Obama, Eric H. Holder Jr., and Michael S. Rogers, who have been sued in their official capacities. The other defendants-appellants are the National Security Agency and the U.S. Department of Justice. Defendants-appellees are Lowell C. McAdam, and Verizon Communications. On February 12, 2014, Lowell McAdam and Verizon Communications notified this Court that they would not be participating in the appeal. This Court has granted the motion of the Center for National Security Studies to participate in this appeal as amicus curiae.

This Court has consolidated No. 14-5004 and 14-5016 with No. 14-5005 and its cross-appeal, No. 14-5017. Nos. 14-5005 and 14-5017 are appeals from the district court's order entered in 13cv881. In that case, plaintiffs-appellees (and cross-appellants) are Larry Elliot Klayman, Michael Ferrari, Charles Strange, and Matt Garrison. Defendants-appellants (and cross-appellees) include Eric H. Holder, Jr., Barack Hussein Obama, and Michael S. Rogers, who have been sued in their official capacities. The other defendants-appellants are the National Security Agency and the U.S. Department of Justice. Defendants-appellees are Facebook, Mark Zuckerberg, Google, Inc., Larry Page, Youtube LLC, Salar Kamangar, Apple, Timothy Cook, Microsoft, Steve Ballmer, Skype, Tony Bates, AOL, Tim Armstrong, Yahoo! Inc., Marissa Meyer, PalTalk, Jason Katz, AT&T, Randall L. Stephenson, Sprint Communications Co., and Daniel Hesse. Steven D. Leonard moved in district court for leave to file a brief as amicus curiae.

B. Ruling Under Review

The ruling under review is Judge Richard J. Leon's opinion and order of December 16, 2013, which is reported at 957 F. Supp. 2d 1

(D.D.C. 2013). The district court entered the identical opinion and order in Nos. 13cv851 and 13cv881.

C. Related Cases

Two other related cases are pending in district court challenging alleged government intelligence-gathering programs: 14cv92, and 14cv262.

/s/ Henry C. Whitaker
Henry C. Whitaker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page**

*Authorities upon which we chiefly rely are marked with asterisks.

Constitution

Statutes

Other Authorities

GLOSSARY

3/27 President Statement	Statement by the President on the Section 215 Bulk Metadata Program, http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program.
6/20 AG-DNI Joint Statement	Joint Statement From the ODNI and DOJ on the Declassification of Renewal of Collection Under Section 501 of FISA, http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1082-joint-statement-from-the-odni-and-doj-on-the-declassification-of-renewal-of-collection-under-section-501-of-fisa.
App.	Appendix
March 2014 FISC Op.	*In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-01 (FISC Mar. 20, 2014)

May 2014 Shea Decl.	Decl. of Teresa H. Shea, *Klayman* v. *Obama*, No. 13cv851 (filed May 9, 2014)
June 19 Primary Order	*In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-96 (FISC June 19, 2014)

STATEMENT OF JURISDICTION

Plaintiffs' complaints invoked the district court's jurisdiction under 28 U.S.C. § 1331. *See* App. 39, 74. The district court entered an order partially granting and partially denying plaintiffs' motion for a preliminary injunction. *Klayman* v. *Obama*, 957 F. Supp. 2d 1, 9-10 (D.D.C. 2013). In particular, the district court granted plaintiffs' motion to enjoin preliminarily the operation of the government's Section 215 bulk telephony-metadata program, by requiring the government to destroy any metadata associated with the personal telephones of two subscribers, and prohibiting any future collection of such metadata. *Id.* at 8, 10. The Court stayed that order pending appeal. *Id.* at 10. This Court has appellate jurisdiction under 28 U.S.C. § 1292(a)(1) to review the district court's interlocutory order partially granting and partially denying injunctive relief.

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 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 judicial authorization, conducts targeted electronic queries of that assembled database of 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 presented are:

1. Whether the district court correctly concluded that plaintiffs have standing to challenge the Section 215 bulk telephony-metadata program.

2. Whether the district court correctly concluded that plaintiffs were likely to succeed on their claim that the Section 215 bulk telephony-metadata program violates the Fourth Amendment.

3. Whether the district court correctly concluded that the balance of equities favored imposition of a preliminary injunction against the operation of the Section 215 program.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

I. NATURE OF THE CASE

Plaintiffs brought two related cases challenging the lawfulness of certain government antiterrorism intelligence-gathering activity. In Nos. 14-5004, 14-5016 (No. 13cv851 in district court), plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange brought a putative class-action suit challenging the lawfulness of the government's alleged acquisition and use of bulk telephony metadata from telecommunications providers. App. 35-36. Plaintiffs alleged that these activities violated the First, Fourth, and Fifth Amendments to the Constitution and exceeded the government's statutory authority, and they sought injunctive relief. Plaintiffs also sought to hold a variety of government officials and private individuals personally liable in damages for common law and statutory torts, as well as for alleged constitutional violations. App. 45-56.

In Nos. 14-5005, 14-5017 (No. 13cv881 in district court)—which this Court has consolidated with Nos. 14-5004 and 14-5016—plaintiffs Larry Klayman, Michael Ferrari, Charles Strange, and Matt Garrison

brought a putative class action suit against the government, government officials in their individual capacities, and various private companies and individuals. The complaint challenged what it characterized as the government's "PRISM" surveillance program, which, plaintiffs alleged, encompassed not only the acquisition of telephony metadata from telecommunications companies, but also the content of telephone communications, as well as the content and associated metadata of Internet-based communications, such as e-mail. App. 76-77. Plaintiffs claimed violations of the First, Fourth, and Fifth Amendments, and they sought injunctive relief. Plaintiffs also sought damages from the government, government officials in their individual capacities, and both private individuals and companies for a range of statutory and common law torts, as well as for alleged constitutional violations. App. 80-91.

On October 29, 2013—nearly five months after the early-June filing of their initial complaints in both district court matters, *see* App. 5-6, 24-25—plaintiffs filed identical motions for preliminary injunctions in both district court cases. Those motions sought to "bar[] Defendants from collecting Plaintiffs' call records under the mass call surveillance

program"; to require the government to "destroy all of Plaintiffs' call records already collected under the program" and to prevent the government from "querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs." App. 95, 112.

Construing those motions as limited to the government's Section 215 bulk telephony-metadata program, the district court partially granted and partially denied preliminary injunctive relief. 957 F. Supp. 2d at 8 & n.6. The district court stayed its preliminary injunction pending appeal. *Id.* at 10.

The government appealed the district court's orders in both cases. App. 588, 590. Plaintiffs cross-appealed in both cases. App. 592, 594. This Court has consolidated both sets of appeals.

In the months following the district court's order, the President announced, and the Foreign Intelligence Surveillance Court adopted, changes to the Section 215 bulk telephony-metadata program that further enhanced the program's privacy protections and safeguards.

II. STATUTORY BACKGROUND

The government appeals from a preliminary injunction against the operation of an important facet of the government's intelligence-gathering capabilities aimed at combating international terrorism—a bulk telephony-metadata program the government operates 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." *Id.* § 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 establishes specific procedures for congressional oversight. 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, for example, the date and time a call was made, what number a telephone called or received a call from, and the duration of a call. App. 203. 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. App. 203.

As described in more detail below, the district court enjoined the operation of the Section 215 telephony-metadata program, based on that court's assessment of the program as it existed in December 2013. In January 2014, however, the President announced, and the Foreign

Intelligence Surveillance Court subsequently implemented, changes to the program to make even more robust the program's privacy protections and safeguards.

Under the current version of the Section 215 bulk telephony-metadata program, the government consolidates the metadata provided by the companies into a database that includes a repository of 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." *See, e.g.*, App. 132 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. For example, the record does not support the district court's conclusions that the program collects "the phone metadata of every telephone user in the United States," or that "all phone companies" necessarily participate in the Section 215 program. *Klayman*, 957 F. Supp. 2d at 33; *see id.* at 39 (characterizing the program as effecting "continuous, daily searches of

virtually every American"). Nor are those conclusions correct. *See* Decl. of Teresa H. Shea ¶ 8, *Klayman* v. *Obama*, No. 13cv851 (filed May 9, 2014) ("May 2014 Shea Decl.").[1]

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

---

[1] We explain below that the government should prevail as a matter of law even if the scope of the program were as the district court believed. The May 2014 Shea declaration is included in the Addendum.

[2] http://www.dni.gov/files/documents/0627/BR%2014-96_Primary_Order.pdf. This document is included in the Addendum for the Court's convenience.

must approve in advance the government's use of query terms under that reasonable, articulable suspicion standard. *Id.* at 7-8.[3] This 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. App. 206. 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 37 times in court orders

[3] Before the changes to the program announced by the President in January 2014, Foreign Intelligence Surveillance Court orders permitted the government to conduct queries of the metadata that would show contacts within three steps of the suspected-terrorist selector. App. 204-05. In addition, the prior version of the program permitted the government to query the database using selectors if National Security Agency officials determined that the selector was reasonably suspected of association with a terrorist organization. App. 208.

issued by sixteen different judges.[4] Most recently, the Foreign Intelligence Surveillance Court reauthorized the Section 215 telephony-metadata program on June 19, 2014, in an order that expires on September 12, 2014.[5]

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) and (g). Consistent with that requirement, the Foreign Intelligence Surveillance Court orders authorizing the program require the government to implement comprehensive minimization procedures. App. 207-09; *see generally* June 19 Primary Order. Those procedures

---

[4] App. 202-03; *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; *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-67 (FISC Mar. 28, 2014); *available at* http://www.dni.gov/files/documents/0627/BR_14-67_Primary_Order.pdf; June 19 Primary Order.

[5] *See* June 19 Primary Order. The Director of National Intelligence declassified the fact of that reauthorization on June 20, 2014. *See* http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1082-joint-statement-from-the-odni-and-doj-on-the-declassification-of-renewal-of-collection-under-section-501-of-fisa. ("6/20 AG-DNI Joint Statement")

include the requirement that the government 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 previously identified to the Foreign Intelligence Surveillance Court as the subject of a counterterrorism investigation. App. 204, 208; June 19 Primary Order 7-8, 12.

The vast majority of the metadata is never reviewed by any person; in 2012, for example, government analysts used 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. App. 205. In 2013, that figure was slightly higher but still only 423.[6] 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 Primary Order 7-8, 12.[7] The telephony metadata returned from a query do not include the identities of individuals; the content of any calls; or the name,

---

[6] http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

[7] The first step represents an immediate contact of the suspected-terrorist selector; the second step represents an immediate contact of a first-step contact. App. 205.

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 in the first place. App. 203. 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. App. 208, 246.

The government does not compile comprehensive records or dossiers, even on suspected terrorists, from Section 215 telephony metadata. App. 207. 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. App. 207. The Foreign 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. App. 207-08. The National Security Agency disseminates under the Section 215 program only the tiny fraction of metadata that are themselves associated with suspected-terrorist activity, or are responsive to queries using those suspected-terrorist selectors. App. 208. Subject to those constraints, the result of this analysis provides information the government may use in counterterrorism 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 congressional intelligence committees. App. 209. 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. App. 248-49.

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. Prior to those modifications, and thus at the time the district court entered its injunction, 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. App. 208. 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. App. 205.

In January 2014, the President announced that he was "ordering a transition" that will "end" the "bulk metadata program as it currently exists." Remarks by the President on Review of Signals Intelligence,

http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence. The President announced two modifications to the Section 215 program: limiting analyst review of telephony-metadata query results to contacts within two steps (rather than three) of the suspected-terrorist selector, and requiring 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 approve the selector). In February, the Foreign Intelligence Surveillance Court granted the government's motion to implement those two changes to the program. *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-01 (FISC Feb. 5, 2014).[8]

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

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

215 bulk telephony-metadata program. Statement by the President on the Section 215 Bulk Metadata Program, http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadata-program ("3/27 President 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." Instead of the government obtaining business records of telephony metadata in bulk, the President proposed that telephony metadata should remain in the hands of telecommunications companies. The President stated that "legislation will be needed to permit the government to obtain this information with the speed and in the manner that will be required to make this approach workable." Under such legislation, the government would be authorized to obtain from companies telephony metadata within two steps of Foreign Intelligence Surveillance Court-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 two orders reauthorizing the program with the President's two modifications. *See* 6/20 AG-DNI Joint Statement.

III. PROCEEDINGS BELOW

A. These Suits

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.

App. 250-51. That order expired on July 19, 2013. App. 253. 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. ¶ 7.

Plaintiffs in these consolidated cases are five individuals who allege they are customers of certain telecommunications and Internet companies (not including Verizon Business Network Services). Shortly after the June 2013 unauthorized public disclosure of the Verizon Business Network Services secondary order, plaintiffs brought two related district-court cases challenging the lawfulness of certain government antiterrorism intelligence-gathering activity. In Nos. 14-5004, 14-5016 (No. 13cv851 in district court), plaintiffs Larry Klayman, Charles Strange, and Mary Ann Strange brought a putative class-action

suit challenging the lawfulness of the government's alleged acquisition and use of bulk telephony metadata from telecommunications providers under Section 215. App. 35-36. Plaintiffs alleged that these activities violated the First, Fourth, and Fifth Amendments to the Constitution, and exceeded the government's statutory authority, and they sought injunctive relief. Plaintiffs also sought damages from a variety of government officials and private individuals for a number of common law and statutory torts, as well as for the alleged constitutional violations. App. 45-56.

In Nos. 14-5005, 14-5017 (No. 13cv881 in district court), plaintiffs Larry Klayman, Michael Ferrari, Charles Strange, and Matt Garrison brought a putative class-action suit against the government, government officials in their individual capacities, and various private companies and individuals. The complaint challenged what it characterized as the government's "PRISM" surveillance program, which, plaintiffs alleged, encompassed not only the acquisition of telephony metadata from telecommunications companies, but also the content of telephone communications, as well as the content and associated metadata of Internet-based communications, such as e-mail.

App. 76-77. Plaintiffs claimed violations of the First, Fourth, and Fifth Amendments, as well as statutory violations, and they sought injunctive relief. Plaintiffs also sought damages from government officials in their individual capacities, and private individuals and companies for a range of statutory and common law torts, as well as for the alleged constitutional violations. App. 80-91.

B. The Preliminary Injunction

On October 29, 2013, plaintiffs filed identical motions for preliminary injunctions in both district court cases, asserting that the government's intelligence-gathering activities were causing them irreparable harm. Those motions sought preliminary relief to "bar[] Defendants from collecting call records under the mass call surveillance program"; to require the government to "destroy all of Plaintiffs' call records already collected under the program"; and to prevent the government from "querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs." App. 95, 112.

Construing those motions as seeking relief limited to the government's Section 215 bulk telephony-metadata program, the

district court in December 2013 partially granted and partially denied preliminary injunctive relief. 957 F. Supp. 2d at 8-10.[9] The district court concluded that the factors required for entry of a preliminary injunction were satisfied here.

The district court first rejected the government's argument that plaintiffs were not likely to succeed on the merits of their claims because they had failed to meet their burden of establishing standing to sue. The district court agreed that three of the plaintiffs lacked standing to challenge the Section 215 telephony-metadata program, because those plaintiffs had not alleged they were subscribers of telephone services by a telecommunications provider. 957 F. Supp. 2d

[9] The district court concluded that it lacked jurisdiction to consider any attempt by plaintiffs to enjoin the government's collection of Internet information as opposed to the bulk collection of telephony metadata under Section 215. The district court noted that the government had discontinued the bulk collection of Internet metadata in 2011. 957 F. Supp. 2d at 8 n.6. And to the extent plaintiffs purport to challenge the collection of Internet information under Foreign Intelligence Surveillance Act authorities that authorize the targeted collection of foreign-intelligence information, plaintiffs lack standing to pursue those claims. *See id.* (citing *Clapper* v. *Amnesty International USA*, 133 S. Ct. 1138 (2013)).

at 8 n.5.[10] But the Court concluded that plaintiffs Larry Klayman and Charles Strange had demonstrated standing to challenge the Section 215 program, because they had alleged that they are subscribers of Verizon Wireless cellular telephone services, and because the government has publicly acknowledged that at one point it had collected such metadata from another entity, Verizon Business Network Services. *Id.* at 26-27. The court thought it irrelevant that Verizon Wireless and Verizon Business Network Services are not the same entity because of the government's representation that the Section 215 program includes

---

[10] The district court also held that the Foreign Intelligence Surveillance Act impliedly precluded plaintiffs' claims that the Section 215 program exceeded the government's statutory authority. *See* 957 F. Supp. 2d at 19-23. Subsequent to the district court's ruling, however, plaintiffs withdrew their statutory claims from these cases. *See* Pls.' Opp. to Gov't Defs.' Partial Mot. to Dismiss at 1, *Klayman* v. *Obama*, No. 13cv851 (Jan. 30, 2014) ("Plaintiffs . . . hereby withdraw their [Administrative Procedure Act] and [Stored Communications Act] claims"); Third Am. Compl. ¶¶ 38-58, *Klayman* v. *Obama*, No. 13cv851 (Feb. 10, 2014) (asserting only constitutional claims); Mot. for Leave to File Second Am. Compl. at 3, *Klayman* v. *Obama*, No. 13cv881 (Jan. 30, 2014) (asserting that the proposed amended complaint "remov[es] the cause of action under the [Administrative Procedure Act]"); Proposed Second Am. Compl. ¶¶ 48-68, *Klayman* v. *Obama*, No. 13cv881 (Jan. 30, 2014) (proposed amended complaint asserting only constitutional claims). Therefore, the statutory claims that plaintiffs raised earlier in the litigation can no longer even arguably be a basis for holding that plaintiffs are likely to succeed on the merits of these cases and cannot support entry of a preliminary injunction.

metadata from "multiple" telecommunications networks, and because the district court understood the database to be "comprehensive." *Id.* at 27. The court also held that plaintiffs suffer a constitutionally cognizable injury each time the government electronically queries the Section 215 database because "plaintiffs' metadata . . . is analyzed, manually or automatically" whenever an electronic query of the database is run—even if plaintiffs' metadata is never seen by any human being as part of a query result. *Id.* at 28.

The court next found that plaintiffs were likely to succeed on their claim that the Section 215 telephony-metadata program violates the Fourth Amendment. In analyzing that claim, the district court considered the program as it operated before the President announced changes in January 2014 generally requiring judicial authorization before querying the Section 215 database, and limiting analysis of query results to two, rather than three, steps away from a suspected-terrorist selector. *See* 957 F. Supp. 2d at 15-18.

The court first rebuffed the argument—which has been accepted by multiple judges of the Foreign Intelligence Surveillance Court and other district court judges—that *Smith* v. *Maryland*, 442 U.S. 735

(1979), establishes that there is no Fourth Amendment privacy interest in telephony metadata voluntarily provided to, or created by, telecommunications companies. 957 F. Supp. 2d at 30-37. *Smith* held that an individual had no cognizable privacy interest in information the government had obtained from a telephone "pen register," which recorded the numbers dialed from Smith's phone. 442 U.S. at 743-44. The Court reasoned that Smith lacked such an interest because he had voluntarily transmitted them to the telephone company, which kept the information in its business records. *Id.* at 742-44.

The district court below agreed that "what metadata *is* has not changed over time" since *Smith* was decided. 957 F. Supp. 2d at 35 (emphasis the district court's). The district court nonetheless adopted the novel conclusion that advances in technology since the Supreme Court decided *Smith*, as well as the larger scale of the Section 215 telephony-metadata program, meant that the Supreme Court's decision "simply does not apply" here. *Id.* at 31; *see id.* at 31-37. The district court thus concluded that collection of telephony metadata under the Section 215 program is a Fourth Amendment "search." *Id.* at 37.

The district court then concluded that obtaining telephony metadata about plaintiffs' calls under the Section 215 program was likely unreasonable under the Fourth Amendment. The court rejected the argument that any infringement of a privacy interest effected by the Section 215 program was reasonable under the standard applicable to searches that serve "special needs" of the government. 957 F. Supp. 2d at 38-39. The court did not deny that the Section 215 program served special government national security and safety needs, but concluded that plaintiffs had cognizable privacy interests that outweighed those needs. *Id.* at 39-41. The court characterized plaintiffs' privacy interest in third-party business records containing call information about them as "very significant." *Id.* at 39. The court expressed "serious doubts" about the efficacy of the metadata program "as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism." *Id.* at 40-41. The court, in particular, faulted the government for not "cit[ing] a single instance in which analysis of the [National Security Agency's] bulk metadata collection actually stopped an imminent attack." *Id.* at 40.

Next, the court ruled that plaintiffs would suffer irreparable injury to their constitutional rights without preliminary relief. 957 F. Supp. 2d at 42.

Finally, the district court held that the balance of the equities weighed in favor of imposing a preliminary injunction. The court reiterated its belief that plaintiffs have significant privacy interests in metadata about their calls contained in business records, and disagreed with the government's assessment of the importance of the Section 215 telephony-metadata program to national security. 957 F. Supp. 2d at 43.

The district court stayed its preliminary injunction pending appeal. 957 F. Supp. 2d at 10.

The government filed notices of appeal of the district court's orders in both district court cases. App. 588, 590. Plaintiffs cross-appealed in both cases. App. 592, 594. This Court has consolidated both sets of appeals.

SUMMARY OF ARGUMENT

The district court preliminarily enjoined the operation of an important government antiterrorism program based on the court's

characterization of that program as an "almost-Orwellian" construct that amasses a "wealth of detail" about individuals, thus enabling "continuous, daily searches of virtually every American citizen without any particularized suspicion." 957 F. Supp. 2d 33, 36, 39. That caricature bears no resemblance to reality.

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 has never collected the call records of all Americans under this program, and does not use the Section 215 database to indiscriminately assemble private details about anyone. Instead, 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 are available for analysis under this program 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 district court erred in entering preliminary injunctive relief against this program, and the injunction should be reversed.

1. Plaintiffs have not established standing to sue or that they would suffer irreparable harm absent preliminary relief. There is no evidence that the government has ever collected any information about plaintiffs' calls under the Section 215 telephony-metadata program. Plaintiffs Klayman and Strange aver that they are subscribers of Verizon Wireless, but provide no evidence that the government has ever acquired any business records from that company under the Section 215 program. The district court relied on the fact that the government has acknowledged that, for several months in 2013, it collected business records containing telephony metadata from Verizon Business Network Services. But that is not the same entity as Verizon Wireless, and plaintiffs and the district court could only speculate about the identities of carriers who have provided in the past, and are providing now, business records under the Section 215 program. There is likewise no evidence to support the district court's further 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.

Plaintiffs likewise have not established standing based on their claims that the Section 215 bulk telephony-metadata program chills their activities—and might chill the activities of those who might want to communicate with them—because they fear that government employees may learn confidential information about plaintiffs' communications. Because only a small fraction of the Section 215 telephony metadata is actually reviewed by any person, plaintiffs' asserted chilling injuries are based on unexplained speculation, and subjective chilling effects grounded in such speculation do not support Article III standing.

2. The district court also erred in concluding that plaintiffs were likely to succeed on their claim that the Section 215 program violates the Fourth Amendment. Every other judge who has decided the question has correctly concluded that the district court's holding conflicts with the Supreme Court's decision in *Smith* v. *Maryland*, 442 U.S. 735 (1979), which held that individuals lack a Fourth Amendment

privacy interest in telephone call record information provided by callers to their telecommunications companies. In concluding otherwise, the district court below relied on the novel logic that changes in technology and differences between the scope of the Section 215 program and that of the pen register arrangement in *Smith* vitiate its holding. That reasoning is a non sequitur, because those changes do not diminish the force of *Smith*'s basic rationale—that telecommunications subscribers relinquish any cognizable privacy interest in information that they voluntarily convey to their telecommunications companies, which is then aggregated and maintained in the business records of those companies. That doctrine is binding law and serves important functions. The notion that plaintiffs' Fourth Amendment privacy interests have been infringed by the Section 215 program is especially implausible, given that it is entirely speculative whether any government analyst has ever reviewed, or ever would review, metadata about plaintiffs' calls.

Even if plaintiffs possessed a cognizable privacy interest in business records consisting of telephony metadata—and they do not—producing those records to the government under Section 215 is

reasonable and permissible under the Fourth Amendment's 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, if any, on legitimate privacy concerns is minimal.

3. The district court abused its discretion in concluding that the balance of the equities tips in plaintiffs' favor. 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. By contrast, plaintiffs have at most a minimal privacy interest in having metadata about their calls removed from the Section 215 database. Moreover, the district court's injunction is inappropriate as preliminary relief because it would apparently require the government to refrain from collecting and to destroy metadata, measures that could not be undone if the government were to prevail in the litigation ultimately.

STANDARD OF REVIEW

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.

In reviewing the grant of a preliminary injunction, this Court considers de novo the district court's legal conclusions. *See Sherley* v. *Sebelius*, 644 F.3d 388, 393 (D.C. Cir. 2011). Any balancing of the preliminary injunction factors is reviewed for abuse of discretion. *Id.*

ARGUMENT

THE DISTRICT COURT ERRED IN ENTERING A PRELIMINARY INJUNCTION AGAINST THE OPERATION OF THE SECTION 215 BULK TELEPHONY-METADATA PROGRAM

A. Plaintiffs Have Not Demonstrated Standing To Challenge The Section 215 Bulk Telephony-Metadata Program

Plaintiffs have not demonstrated that the government has ever collected any telephony metadata associated with any of their calls.

Plaintiffs, moreover, cannot show that any metadata about their calls have ever been, or will ever be, reviewed by government personnel. And plaintiffs have identified no other injury sufficient to confer standing to challenge the Section 215 program.

1. To establish Article III standing, plaintiffs must identify an injury that is "'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Amnesty Int'l*, 133 S. Ct. at 1147 (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.* at 1147.

The Supreme Court's decision in *Amnesty International* is particularly instructive. In *Amnesty*, the plaintiffs 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, noting that this claimed injury rested on a "speculative chain of possibilities," such as whether the government would target their communications for surveillance and whether the government would intercept plaintiffs' communications even if the government targeted them. *See id.* at 1148-52.

2. Here, as in *Amnesty*, plaintiffs' claim to injury as a result of the Section 215 program is based only on speculation. Plaintiffs Klayman and Strange express concern that their communications will be "overheard or obtained" under the Section 215 program and in some unspecified way "used against" them. App. 100, 102, 345. 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).[11] Plaintiffs' asserted future injury rests on an impermissibly speculative causal chain.

First, plaintiffs can only speculate whether the government has ever collected any metadata about them at all. The only support plaintiffs provide for that assumption is their assertion that they are subscribers of Verizon Wireless cellular phone service. App. 98, 101. But there is no evidence in the record that the government has acquired metadata from Verizon Wireless under the Section 215 program. The only telecommunications carrier the government has publicly acknowledged to have received Section 215 production orders is a separate entity, Verizon Business Network Services—the entity that was the subject of the Foreign Intelligence Surveillance Court order that was disclosed publicly without authorization in June 2013.

[11] 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.

The district court did not dispute that those two entities are distinct, but found standing based on its speculation that the government must be collecting metadata from Verizon Wireless because of the government's representation that the Section 215 program operates "across multiple telecommunications networks" and because Verizon Wireless is the nation's largest wireless telecommunications carrier. 957 F. Supp. 2d at 27 (internal quotation marks and emphasis omitted). But the Section 215 telephony-metadata program, though broad in scope, has never encompassed all, or even virtually all, call records and does not do so today. *See* May 2014 Shea Decl. ¶ 8. Contrary to the district court's speculation, it does not follow that the government must under the Section 215 program collect metadata from all of the three "largest carriers" in order for that program to "serve its . . . function." 957 F. Supp. 2d at 27.

3. Even if there were evidence that the government had collected metadata about plaintiffs' telephone calls under the Section 215 program, plaintiffs would still lack standing. Plaintiffs claim injury based on their allegation that the government will "use" metadata about their calls in some unspecified way "against" them. App. 100,

102, 345. Plaintiffs, however, provide no explanation for how those injuries could arise if government personnel never review any metadata about plaintiffs' calls that may be contained in the Section 215 database. 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 generally be an advance judicial finding that a given selector is suspected of association with terrorism, and only the small fraction of metadata responsive to queries using such selectors may ever be reviewed.

Indeed, those protections are even more robust today than they were when the district court entered its preliminary injunction in December 2013. At that time, no judicial finding was required before querying the database; and query results could return metadata within three steps, rather than the current two, of the suspected-terrorist selector. *See* 957 F. Supp. 2d at 16 (stressing that, under the old version of the program, "intelligence analysts, *without seeking the approval of a judicial officer*, may access the" Section 215 database

(emphasis the district court's)); *id.* at 16 n.21 (describing the "spiderweb-like reach of the three-hop search"). Thus, there is only a speculative prospect that metadata about plaintiffs' calls would ever be used as a selector to query, or be among the metadata included in the results of queries of, the telephony metadata.

The district court thought that fact immaterial because it believed that plaintiffs suffer a cognizable Article III injury each time the government queries the database, because all information in it "is analyzed . . . whenever the Government runs a query." 957 F. Supp. 2d at 28.[12] But even if that were true, and it is not because a person never sees the information queried other than the results, the district court did not explain how queries of the database that return no information about plaintiffs would harm them. Nor did the district court elaborate on how metadata that no person reviews could reveal any details—let alone "a wealth of detail," *id.* at 36—about any individual. *See, e.g.*, *Amnesty Int'l*, 133 S. Ct. at 1147 (requiring identification of a "concrete,

[12] The district court cited no allegations or evidence to support this assertion, and there are none.

particularized, and actual or imminent" harm that is "fairly traceable" to the conduct complained of (internal quotation marks omitted)).

In any event, 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, e.g.*, *United States* v. *Place*, 462 U.S. 696, 707 (1983) (canine sniff of luggage does not violate a reasonable expectation of privacy); *Defenders of Wildlife* v. *Perciasepe*, 714 F.3d 1317, 1323 (D.C. Cir. 2013) (injury for Article III standing purposes must be "an invasion of a legally protected interest"). Where telephony metadata associated with particular calls remain unreviewed and never come to any human being's attention, there is no invasion of any cognizable privacy interests, and no injury to support standing to sue.

4. Finally, plaintiffs' asserted injuries are entirely attributable to their subjective, speculative fear that the government may, in some unspecified way, use any information the government possesses about them against them. Both this Court and the Supreme Court have made clear that such amorphous fears are not a basis for challenging a

government intelligence-gathering program. *See Amnesty Int'l*, 133 S. Ct. 1152-53; *Laird* v. *Tatum*, 408 U.S. 1, 10-14 (1972); *United Presbyterian Church* v. *Reagan*, 738 F.2d 1375, 1378-79 (D.C. Cir. 1984) (Scalia, J.,).

In *Presbyterian Church*, for example, the plaintiffs asserted standing to challenge government surveillance practices set forth in an executive order. This Court rejected standing to sue because plaintiffs had not asserted that they "suffered some concrete harm (past or immediately threatened) apart from the 'chill' itself." 738 F.2d at 1378. Here, as in *Presbyterian Church*, plaintiffs have made no attempt to identify any concrete way in which the government may use any metadata about their calls against them, and "no part of the challenged scheme imposes or even relates to any direct governmental constraint upon the plaintiffs." *Id.* at 1380.

Similarly, in *Laird*, the Supreme Court made clear that standing cannot be supported by plaintiffs' speculative fear that the government might "in the future take some *other* and additional action detrimental to" them. 408 U.S. at 11, 13-14. Notably, in *Laird* that was true even though the government had subjected those plaintiffs to surveillance.

See id. at 39 (Brennan, J., dissenting). Plaintiffs' unelaborated fears of unspecified government action create no case or controversy. *See Presbyterian Church*, 738 F.2d at 1380.

B. Plaintiffs Are Not Likely To Succeed On Their Claim That The Section 215 Program Violates The Fourth Amendment

1. The Program Does Not Infringe A Constitutionally Protected Privacy Interest

The Supreme Court has rejected the premise of plaintiffs' 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*, 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. *Smith*, 442 U.S. at 743-44. Except for the district court below, every other court to have decided the matter—including numerous decisions of the Foreign Intelligence Surveillance Court as recently as June of this year—has correctly relied on the holding of *Smith* to conclude that the acquisition from telecommunications companies of business records consisting of bulk telephony metadata is not a search for purposes of the

Fourth Amendment. *See* App. 134, 178; *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.");[13] *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, Dkt. No. BR-14-96 (FISC June 19, 2014);[14] *Smith* v. *Obama*, 2014 WL 2506421, at *4 (D. Idaho June 3, 2014); *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 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

---

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

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

listening device that would permit the government to monitor the content of communication. *Id.* (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 conveys to the phone company. Because telephone users convey numbers to the telephone company to complete their calls, and because the telephone company can and does routinely record those numbers for legitimate 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 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 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 certainty is essential in this area to facilitate compliance with the Constitution. *Id.* at 581-86.

Indeed, the Fourth Amendment interests here are in some respects even weaker than in *Smith*. To begin with, this case concerns business records maintained by telecommunications companies for their own business purposes, whereas the pen register in *Smith* directly intercepted the transmission of information from a subscriber to a telecommunications company. Plaintiffs have no reasonable expectation of privacy in corporate business records. *See Minnesota* v.

Carter, 525 U.S. 83, 88 (1998); *Rakas* v. *Illinois*, 439 U.S. 128, 133-34 (1978).

In *Smith*, moreover, the police targeted information about the phone calls of a single, known individual, ascertained who he was calling, and used that information to arrest and prosecute him. 442 U.S. at 737, 741-42. Here, in contrast, the government may review metadata under the Section 215 program only in extremely restricted circumstances that are not remotely likely to implicate information about plaintiffs' calls.

The district court attempted to distinguish *Smith* on a number of grounds; none is persuasive. First, the district court suggested that the pen register in *Smith* "was operational for only a matter of days," whereas under the Section 215 program the government retains records for a number of years. 957 F. Supp. 2d at 32. *Smith*, however, was explicit that "[t]he fortuity of whether or not the phone company"—which the Court assumed to be an agent of the government, *see* 442 U.S. at 739 n.4—"in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference," *id.* at 745. The greater time period of metadata collected

does not validly distinguish *Smith*, because *Smith* makes clear that no Fourth Amendment privacy interest exists in *any* of the data voluntarily conveyed to a telephone company. The Foreign Intelligence Surveillance Court recently explained, in rejecting the district court's reasoning, 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 district court's attempted distinction makes no difference.

Second, the district court suggested that under the Section 215 program, telecommunications providers "operate what is effectively a joint intelligence-gathering operation" with the government, whereas in *Smith* "a third party" was "collect[ing] information and then turn[ing] it over to law enforcement." 957 F. Supp. 2d at 33. That characterization of the Section 215 program is fictional; in fact, as explained above, the production of a company's own business records is, if anything, less intrusive than the installation of a pen register in *Smith*—particularly where, as here, there is no evidence or reason to believe that records pertaining to plaintiffs' calls have been or ever will be reviewed by government analysts. Under the Section 215 program, the government collects business records from telecommunications providers that the companies themselves maintain. *See* App. 202. The Supreme Court in *Smith* emphasized that it was precisely because a telephone company could and did maintain such call records that an individual has no actual expectation of privacy (let alone a reasonable one) in that information. *See* 442 U.S. at 743 ("Telephone users typically know that they must convey numerical information to the phone company . . . and that the phone company does in fact record this information for a

variety of legitimate business purposes."). In any event, the Supreme Court premised *Smith* on the assumption that the phone company *was* "deemed an 'agent' of the police for purposes of this case." *Id.* at 739 n.4 (internal quotation marks the Court's).

Third, the district court opined that the larger scale of metadata collection enabled by advances in what it characterized as "almost-Orwellian technology" since *Smith* has changed the privacy interests at stake. 957 F. Supp. 2d at 33. That assertion overlooks that Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald* v. *United States*, 451 U.S. 204, 219 (1981); *accord*, *e.g.*, *Carter*, 525 U.S. at 88; *Rakas*, 439 U.S. at 133-34.[15] 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

[15] Thus, plaintiffs cannot invoke the Fourth Amendment rights of others, even if there were a reasonable expectation of privacy in telephony metadata. *See, e.g.*, *Rakas*, 439 U.S. at 137-38; *United States* v. *Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (an individual's Fourth Amendment rights are violated only when the challenged conduct invaded his own legitimate expectation of privacy rather than that of a third party).

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*." App. 137. Accordingly, as the Foreign Intelligence Surveillance Court recently explained in response to the district court's analysis here, "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.*, *United States* v. *Dionisio*, 410 U.S. 1, 13 (1973) (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"); *United States* v. *Rigmaiden*, 2013 WL 1932800, at *13 (D. Ariz.

May 8, 2013) (no Fourth Amendment violation when government acquired 1.8 million IP addresses).[16]

Finally, the district court pointed to the fact that cell phones did not exist in 1979, but are ubiquitous now, and are used for many purposes other than calling, meaning that "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago." 957 F. Supp. 2d at 36. Metadata today, the district court stated, "reflects a wealth of detail about . . . familial, political, professional, religious, and sexual associations," and "reveal an entire mosaic—a vibrant and constantly updating picture of the person's life." *Id.* And the district court pointed out that cell phones today are used as far more than just calling devices; they are also used, for example, as "maps and music players," or as a "lighter[] that people hold up at rock concerts." *Id.* at 34; *see also Riley* v. *California*, 134 S. Ct. 2473, 2489

[16] For these reasons, plaintiffs' Fourth Amendment claim fails regardless of the scope of the business records obtained under the program. The district court's mistaken belief that the Section 215 bulk telephony-metadata program includes all or virtually all of the telephony metadata of Americans thus does not alter the result here. *See supra* p. 10-11. Many details of the program remain classified, but unsupported assumptions about the program cannot justify the extraordinary remedy of preliminary injunctive relief.

(2014) (noting that cell phones today could "just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"). In *Riley*, the Supreme Court recently relied on these many other functions served by cell phones in holding that police generally must obtain a warrant before searching a cell phone seized incident to an arrest. *See Riley*, 134 S. Ct. at 2489-93. But the district court's observation about the capabilities of cell phones and the Supreme Court's decision in *Riley* have no bearing on this case.

The preliminary injunction under review in these appeals concerns solely telephony metadata and has nothing to do with uses for cell phones beyond calling.[17] As to that use, even the district court

[17] The Supreme Court made clear in *Riley* that "[b]ecause . . . these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." 134 S. Ct. 2489 n.1 (emphasis the Court's). The question here, by contrast, is whether obtaining telephony metadata is a "search" at all. *See id.* at 24 (refusing to apply *Smith* because "[t]here is no dispute here that the officers engaged in a search"). The purpose and operation of the Section 215 telephony-metadata program, moreover, differ critically from the searches of a cell phone's content incident to arrest in *Riley*. For example, the Section 215 telephony-metadata program is conducted pursuant to orders issued by the

Continued on next page.

agreed that "what metadata *is* has not changed over time." 957 F. Supp. 2d at 35 (emphasis the district court's). Telephony metadata—the numbers a person dials to make a call, and associated information recorded by telecommunications providers, such as the date, time, and duration of the call—could reveal details about individuals in 1979 no less than today.[18] Other business records subject to the third-party doctrine likewise reflect a breadth of personal information. For example, the checks, deposit slips, and other customer bank records at issue in *Miller*—a case on which *Smith* relied—surely revealed a variety of personal details. *See* 442 U.S. at 743 (citing *United States* v. *Miller*, 425 U.S. 435, 442-44 (1976). That point was not lost on the dissenting Justices in both *Smith* and *Miller*, *see Smith*, 442 U.S. at 748 (Stewart, J., dissenting); *Miller*, 425 U.S. at 451 (Brennan, J., dissenting), yet the

---

Foreign Intelligence Surveillance Court, and review of the metadata requires a showing of reasonable suspicion, whereas the cell-phone searches at issue in *Riley* were conducted without any judicial authorization or threshold showing of suspicion.

[18] The Eleventh Circuit recently held that the collection of cell-site location information can implicate a Fourth Amendment privacy interest. *See United States* v. *Davis*, __ F.3d __, 2014 WL 2599917, at *9-*10 (11th Cir. June 11, 2014). The Section 215 telephony-metadata database does not contain cell-site location information. *See* App. 203. The government is considering whether to seek further review of the *Davis* decision.

Supreme Court in both cases applied the third-party doctrine to hold that any reasonable expectation of privacy was forfeited when customers provided that information to their bank or telephone company. There is no reason to reach a different result with regard to the Section 215 program; as the Foreign Intelligence Surveillance Court observed, "[i]t is far from clear . . . that even years' worth of non-content call detail records would reveal more of the details about a telephone user's personal life than several months' worth of the same person's bank records." March 2014 FISC Op. at 21.

The district court's portrayal of the privacy interests at stake, furthermore, overlooks the carefully crafted safeguards embedded into the Section 215 program, which are designed to avoid indiscriminately yielding a "wealth of detail" about individuals. The governing Foreign Intelligence Surveillance Court orders require specified telecommunications companies to turn over only limited information from their business records under Section 215; that telephony metadata does not include the identity of any particular subscriber or called party. App. 203. The current restrictions imposed by Foreign Intelligence Surveillance Court orders permit access only to telephony

metadata that is within two steps of a selector for which there is a reasonable, articulable suspicion (now founded on a prior judicial determination except in exigent circumstances) of association with a terrorist organization. June 19 Primary Order 7-8, 12. Those protections are even more robust than those the district court considered when it entered its injunction in December 2013, when such a judicial finding was not generally required before querying the database, and when analysts could examine metadata within three steps, rather than the current two, of a selector. *See* 957 F. Supp. 2d 15-18. There is thus even less basis today for the district court's assumption that this program reveals private details about millions of individuals. And it bears emphasizing that these "strict protections . . . do not apply to run-of-the-mill productions of similar information in criminal investigations." March 2014 FISC Op. at 22.

Contrary to the district court's apparent assumptions, *Smith*'s principles have guided Fourth Amendment decisions even as to forms of communication that did not exist when the Supreme Court handed down *Smith* in 1979. *See, e.g.*, *United States* v. *Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (email "to/from" and Internet Protocol addressing

information); *Quon* v. *Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008) (text message address information), *rev'd on other grounds*, 560 U.S. 746 (2010); *Guest* v. *Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (subscriber information such as names, addresses, birthdates, and passwords communicated to systems operators and Internet service providers). This case is more straightforward: it involves telephony metadata, which is the same type of information that was at issue *Smith*.

The district court also emphasized the larger volume of metadata about each person's calls that is involved in the Section 215 program, in an effort to distinguish it from *Smith*, and compared that difference to the difference between short-term and long-term GPS monitoring. 957 F. Supp. 2d. at 30-31. But that comparison is inapt.

In *United States* v. *Knotts*, 460 U.S. 276 (1983), the Supreme Court held that the short-term use of a tracking beeper infringes no legally protected privacy interest because an individual has no expectation of privacy in his public movements. *Id.* at 281-82. In *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),

however, this Court held that an individual could nonetheless have a privacy interest in long-term GPS monitoring of his movements because GPS monitoring enables the government to aggregate private details of an individual's life in a way that could not easily be done by a stranger "because the likelihood a stranger would observe all those movements . . . is essentially nil," 615 F.3d at 560—a conclusion echoed by concurring Justices in *United States* v. *Jones*. *See* 132 S. Ct. at 955-56 (Sotomayor, J., concurring); *id.* at 962-64 (Alito, J., concurring in the judgment). But the Supreme Court in *Smith*, as this Court noted in *Maynard*, recognized that telephony metadata in the business records of telecommunications providers is indeed aggregated: unlike an individual's public movements, an individual "expects all the numbers he dials to be compiled in a list" maintained by the telephone company. *Maynard*, 615 F.3d at 561 (citing *Smith*, 442 U.S. at 742-43). Even if there are more phone calls now than in 1979, the relevant expectation concerning telephony metadata conveyed to a telecommunications carrier is not materially different. Moreover, unlike GPS data, information in the Section 215 telephony-metadata database is not indiscriminately compiled about individuals; rather, the telephony

metadata may be reviewed only as part of the highly restricted process of querying. Again, plaintiffs have not shown, and it is not remotely likely, that metadata about plaintiffs' calls have ever been, or ever will be, the subject of, or responsive to, such a query.

Given the conclusive, controlling effect of *Smith*, plaintiffs are not likely to succeed on the merits of their Fourth Amendment claim.

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

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); *Hartness* v. *Bush*, 919 F.2d 170, 173 (D.C. Cir. 1990). The national security and safety interests served by the Section 215 program are special needs of the utmost importance. *See Hartness*, 919 F.2d at 173; *Cassidy* v. *Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006);

MacWade v. *Kelly*, 460 F.3d 260, 270-71 (2d Cir. 2006) (citing *Michigan Department of State Police* v. *Sitz*, 496 U.S. 444 (1990)).

The government has shown, and the Foreign Intelligence Surveillance Court has repeatedly concluded, that 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, including connections that retrospective analysis can make evident in calls that occurred before the relevant terrorist connection became known. The Foreign Intelligence Surveillance Court orders authorizing the Section 215 bulk telephony-metadata program authorize 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. App. 213-17, 230-31.

In light of the imperative national-security interests the program serves and the numerous privacy protections that the Foreign

Intelligence Surveillance Court has required 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 quotation marks omitted). The interest in preventing international 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 unknown terrorist operatives who could otherwise elude detection, and has meaningfully contributed to counterterrorism investigations. App. 213-16, 229-30.

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 non-speculative basis to believe that any information concerning plaintiffs' calls—or those of the vast bulk of other telephone subscribers—has been or will ever be seen by any person. App. 205-06, 207-09. *See King*, 133 S. Ct. at 1979 (finding no Fourth Amendment violation where safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Board 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 in a database; the information is then only accessed as part of the highly restricted querying process, which requires judicial approval under a reasonable suspicion standard.

The record amply establishes that the Section 215 bulk telephony-metadata program, coupled with the targeted and judicially supervised querying of that metadata, is at least a "reasonably effective means" of promoting the government's national security objectives. *Earls*, 536 U.S. at 837. Indeed, courts have upheld searches on national security grounds that were arguably more intrusive. *See Cassidy*, 471 F.3d at 70 (searches of carry-on luggage and vehicles before boarding ferries); *MacWade*, 460 F.3d at 270-71 (random search of subway passengers' baggage).

The district court minimized the importance of the Section 215 telephony-metadata program, faulting the government for providing no "instance in which analysis of . . . bulk metadata collection actually stopped an imminent attack." 957 F. Supp. 2d at 40. But the Fourth Amendment plainly does not require the government to demonstrate that special-needs searches—often one tool of many that promote security and safety—have prevented such specific harms, particularly where, as here, plaintiffs' cognizable privacy interests are minimal. *See Nat'l Treasury Emps.* v. *Von Raab*, 489 U.S. 656, 675 n.3 (1989) ("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"). Nor was the district court correct to downplay the significance of the Section 215 program in enabling the government to conduct historical analysis, contact-chaining, and timely identification of terrorist contacts. 957 F. Supp. 2d at 40. The ability to analyze quickly past connections and chains of communications to determine terrorist connections can serve important interests in the midst of an active terrorism investigation. The record reflects the views of government officials that the program is a valuable counterterrorism tool. *E.g.*, App. 212-18, 223, 226-30. The President also has stressed the "importance of maintaining this capability." 3/27 President Statement. 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 the district court'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"). And while the President has expressed support for legislation to modify the Section 215 program, under which the government would no longer obtain telephony metadata in bulk, the goal remains, at the same time, to preserve the capabilities needed to accomplish the program's objectives. *See*, *e.g.*, 3/27 President Statement. The importance of preserving that capability only underscores the important function served by the Section 215 program in its current form.

C. The District Court Abused Its Discretion In Balancing The Equities And Assessing The Public Interest

Neither the public interest nor the balance of the equities supports a preliminary injunction against the Section 215 telephony-metadata program, and the district court abused its discretion in concluding otherwise.

As an initial matter, even if, contrary to the government's contention, plaintiffs have some cognizable Article III interest in enjoining the Section 215 telephony-metadata program, that interest is surely minimal, particularly given the remote likelihood that metadata pertaining to their calls would ever be reviewed by a human being. On

the other side of the ledger, the government has a substantial interest in continuing the Section 215 program, a valuable tool in the government's antiterrorism arsenal, for reasons already explained.

The district court did not dispute "the public's interest in combating terrorism," but thought that entering a preliminary injunction would not diminish that interest because the preliminary injunction bars the government from collecting telephony metadata only regarding plaintiffs Klayman and Strange, and requires the government to destroy any metadata it possesses only regarding those two individuals. 957 F. Supp. 2d. at 43. The government has explained, however, that, for technological and practical reasons, complying with those demands could ultimately have a degrading effect on the overall program and would consume considerable resources. App. 218. Moreover, requiring the government to refrain from collecting and to destroy records regarding those plaintiffs would be irreversible, and hence is wholly improper preliminary injunctive relief, because it effectively grants plaintiffs 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 preliminary injunction should be reversed.

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN JR.
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

JULY 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 12,517 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

CERTIFICATE OF SERVICE

I hereby certify that on July 14, 2014, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. I further certify that I will cause 8 paper copies of this brief to be filed with the Court within two business days.

/s/ Henry C. Whitaker
HENRY C. WHITAKER