[NOT YET SCHEDULED FOR ORAL ARGUMENT]

Nos. 14-5004, 14-5005, 14-5016, 14-5017 (Consolidated)

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

BRIEF *AMICI CURIAE* OF THE ELECTRONIC FRONTIER FOUNDATION, THE AMERICAN CIVIL LIBERTIES UNION, AND THE ACLU OF THE NATION'S CAPITAL IN SUPPORT OF APPELLEES

Counsel for Amici Curiae :
Mark Rumold
Andrew Crocker
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
mark@eff.org

Of Counsel:
Alex Abdo
Patrick Toomey
Jameel Jaffer
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
aabdo@aclu.org

Arthur B. Spitzer
American Civil Liberties Union of the Nation's Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, DC 20008
Phone: (202) 457-0800
artspitzer@aclu-nca.org

STATEMENT REGARDING CONSENT TO FILE AND SEPARATE BRIEFING

Pursuant to D.C. Circuit Rule 29(b), undersigned counsel for *amici curiae* the Electronic Frontier Foundation ("EFF"), the American Civil Liberties Union ("ACLU"), and the American Civil Liberties Union of the Nation's Capital ("ACLU-NCA") represents that all parties have consented to the filing of this brief.[1] Pursuant to D.C. Circuit Rule 29(d), undersigned counsel certifies that separate briefing is necessary. EFF, ACLU and ACLU-NCA are civil liberties organizations well-suited to discuss the technical and constitutional issues raised by the government's collection of telephone records, issues not covered by the other *amicus* brief expected to be filed in this case.

[1] Pursuant to Fed. R. App. P. 29(c), counsel for *amici curiae* states that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae* or their counsel made a monetary contribution to its preparation or submission.

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rule 26.1 and Federal Rule of Appellate Procedure 26.1, *amici curiae* state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

Pursuant to D.C. Circuit Rule 28(a)(1), *amici curiae* certify that:

A. Parties and Amici

Except for the EFF, ACLU, and ACLU-NCA and any other *amici* who have not yet entered an appearance in this proceeding, all parties, *amici* and intervenors appearing in the court below and before this Court are listed in the Brief for the Appellants.

B. Rulings Under Review

References to the rulings at issue appear in the opening Brief for the Appellants.

C. Related Cases

References to the related cases appear in the Brief for the Appellants.

D. Statutes and Regulations

All applicable statutes and regulations are contained in the Brief for the Appellants.

TABLE OF CONTENTS

STATEMENT REGARDING CONSENT TO FILE AND SEPARATE BRIEFING i

CORPORATE DISCLOSURE STATEMENT ii

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES iii

TABLE OF CONTENTS iv

TABLE OF AUTHORITIES vi

GLOSSARY OF ABBREVIATIONS x

STATEMENT OF INTEREST 1

INTRODUCTION 2

ARGUMENT 3

I. METADATA REVEALS HIGHLY PERSONAL AND SENSITIVE INFORMATION 3

A. Telephony Metadata Reveals Sensitive Information, Even in Limited Quantities 7

B. In the Aggregate, Telephony Metadata Is Even More Revealing 8

C. Creating a Trail of Sensitive Metadata Is an Unavoidable Byproduct of Modern Life 12

II. THE BULK COLLECTION OF TELEPHONE RECORDS VIOLATES INDIVUDUALS' REASONABLE EXPECTATION OF PRIVACY 15

A. *Smith* Does Not Authorize the Bulk Collection of Revealing Personal Information Such as Telephony Metadata 17

B. Dragnet Collection of Highly Revealing Information Is a Fourth Amendment "Search" 22

CONCLUSION 29

TABLE OF AUTHORITIES*

Federal Cases

ACLU v. Clapper,
959 F. Supp. 2d 724 (S.D.N.Y. 2013),
appeal pending, No. 14-42 (2d Cir. filed Jan. 2, 2014) 1, 7

Bond v. United States,
529 U.S. 334 (2000) 21

Chapman v. United States,
365 U.S. 610 (1961) 20

Chimel v. California,
395 U.S. 752 (1969) 26

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 20

First Unitarian Church of Los Angeles, et al. v. NSA, et al.,
No. 13-cv-03287 JSW (N.D. Cal. July 16, 2013) 1

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted],
No. BR 13-109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013) 5, 9

Katz v. United States,
389 U.S. 347 (1967) 17, 27

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013) 18, 19, 27

Kyllo v. United States,
533 U.S. 27 (2001) 16

**Riley v. California*,
134 S. Ct. 2473 (2014) 18, 25, 26, 27, 28

* *Authorities chiefly relied upon are indicated with asterisks.*

Smith v. Maryland,
442 U.S. 735 (1979) 2, 3, 12, 16, 17, 18, 19, 21, 22, 27

Stoner v. California,
376 U.S. 483 (1964) 20

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013 (en banc) 22, 26, 27

United States v. Davis,
754 F.3d 1205 (11th Cir. 2014) 22, 24, 27

United States v. Flores-Montano,
541 U.S. 149 (2004) 27

United States v. Forrester,
512 F.3d 500 (9th Cir. 2008) 19, 20, 22

**United States v. Jones*,
565 U.S. __, 132 S. Ct. 945 (2012) 2, 21, 23, 24, 25, 27

United States v. Knotts,
460 U.S. 276 (1983) 2, 22, 23, 25, 27

**United States v. Maynard*,
615 F.3d 544 (D.C. Cir. 2010)..... 3, 23, 24, 25, 27

United States v. Miller,
425 U.S. 435 (1976) 21

United States v. Robinson,
414 U.S. 218 (1973) 26

United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div. ("Keith"),
407 U.S. 297 (1972) 15

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 21, 22

United States v. Young,
573 F.3d 711 (9th Cir. 2009) 21

Federal Statutes

18 U.S.C. § 2703 6

18 U.S.C. § 2709 6

Section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861 5

Constitutional Provisions

U.S. Const., amend. IV 3, 15, 16, 21, 22, 23, 25, 26, 28

Other Authorities

Carter Jernigan and Behram Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, First Monday (Oct. 5, 2009) 14

Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research 11

Corrina Cortes, *et al*., *Communities of Interest*, AT&T Shannon Research Labs .. 11

Eunjoon Cho, *et al*., *Friendship and Mobility: User Movement In Location-Based Social Networks* (2011) 14

James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times (Sep 28, 2013) 13

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA's Got Your Number* (Dec. 23, 2013) 6

Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014) 8, 12

Letter from Nat'l Sec. Agency Legislative Affairs Office to Senate Select Committee on Intelligence (Dec. 1, 2010) 5

Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013) 9, 13

Matt Blaze, *Phew, NSA is Just Collecting Metadata. (You Should Still Worry)* Wired (June 19, 2013) 9

Michael Kosinski, *et al.*, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l. Acad. Sci 5802 (2013)..... 14

Nat'l Research Council of the Nat'l Academies of Sci., *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (2008). 13

Privacy and Civil Liberties Oversight Bd., Report on the Telephone Records Program (Jan. 23, 2014) 6, 10, 28

Richard Becker, *et al.*, *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, AT&T Labs-Research 11

Rodrigo de Oliveira, Alexandros Karatzoglou, Pedro Concejero, Ana Armenta & Nuria Oliver, Towards a Psychographic User Model from Mobile Phone Usage, CHI 2011 Work-in-Progress (May 7–12, 2011)..... 12

Siobhan Gorman, *et al.*, *U.S. Collects Vast Data Trove*, Wall St. J. (June 7, 2013) 9

Steven M. Bellovin, *Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the § 215 and § 702 Surveillance Programs* (July 31, 2013)..... 5

Transcript of President Obama's Jan. 17 Speech on NSA Reforms, Wash. Post (Jan. 17, 2014) 3

Transcript: Dianne Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program, Wash. Post (June 6, 2013)..... 3

Yaniv Altshuler, *et al.*, *Incremental Learning with Accuracy Prediction of Social and Individual Properties from Mobile-Phone Data* (2012)..... 15

Yves-Alexandre de Montjoye, *et al.*, *Unique in the Crowd: The Privacy Bounds of Human Mobility* (2013) 15

GLOSSARY OF ABBREVIATIONS

IMEI	Internal Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
PCLOB	Privacy and Civil Liberties Oversight Board

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization working to protect innovation, free speech, and privacy in the online world. With more than 27,600 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. EFF represents the plaintiffs in *First Unitarian Church of Los Angeles*, *et al. v. NSA*, *et al*., No. 13-cv-03287 JSW (N.D. Cal. July 16, 2013), which also involves a challenge to the government's collection of Americans' telephone records.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The American Civil Liberties Union of the Nation's Capital ("ACLU-NCA") is the Washington, D.C. affiliate of the ACLU. The protection of individual privacy from government intrusion as guaranteed by, among other authorities, the Fourth Amendment is an area of particular concern to the ACLU and its affiliates, which have been involved as counsel for parties or as *amici* in many cases involving those issues. In particular, the ACLU is a plaintiff in *ACLU v. Clapper*, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013), *appeal pending*, No. 14-42 (2d Cir. filed Jan. 2, 2014), which presents very similar issues to those presented here.

INTRODUCTION

Telephony metadata reveals private and sensitive information about people. It reveals political affiliation, religious practices, and people's most intimate associations. It reveals who calls a suicide prevention hotline and who calls their elected official; who calls the local Tea Party office and who calls Planned Parenthood. The aggregation of telephony metadata—about a single person over time, about groups of people, or with other datasets—only intensifies the sensitivity of the information. Aggregated metadata "generates a precise, comprehensive record" of people's habits, which in turn "reflects a wealth of detail about [their] familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. __, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). The call records collected by the government are not *just* metadata—they are intimate portraits of the lives of millions of Americans.

The privacy concerns raised by the bulk collection of telephony metadata cannot be assuaged by reliance on *Smith v. Maryland*, 442 U.S. 735 (1979). The nature and scope of the telephone records program at issue here, and the revealing insights it is capable of generating, are so thoroughly different from the holding in *Smith* that the case simply does not apply. As the Supreme Court recognized in *United States v. Knotts*, 460 U.S. 276 (1983), just four years after deciding *Smith*, and as this Court more recently recognized in *United States v. Maynard*, 615

F.3d 544 (D.C. Cir. 2010), dragnet surveillance is fundamentally different than targeted collection. It raises Fourth Amendment questions distinct from—and more profound than—those presented in *Smith* and related cases, and it requires its own consideration.

In light of that consideration, *amici* urge this Court to uphold the district court and hold that the bulk collection of telephony metadata violates the Fourth Amendment.

ARGUMENT

I. METADATA REVEALS HIGHLY PERSONAL AND SENSITIVE INFORMATION.

In an attempt to alleviate concerns about the NSA's call record collection program, Senator Dianne Feinstein, the Chair of the Senate Select Committee on Intelligence, said: "As you know, this is just metadata. There is no content involved."[2] Her sentiment echoes views expressed by President Obama, as well as the position advanced by the government in this case.[3] Implicit in this view is the

[2] *Transcript: Dianne Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, Wash. Post (June 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program.

[3] *Transcript of President Obama's Jan. 17 Speech on NSA Reforms,* Wash. Post (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html. ("Let me repeat what I said when this story first broke. This program does not involve the content of phone calls or the names of people

suggestion that "content" is sensitive (and its collection worthy of concern), but "metadata" is not (and should raise no alarm). *Amici* hope to disabuse the Court of this notion. The pool of telephony metadata collected by the government reveals a wealth of deeply personal and intimate information about millions of Americans. Its sensitivity cannot be discounted.

At the outset, it bears emphasizing that there is nothing axiomatic or particularly profound about defining specific sets of communications data as "metadata" as opposed to "content." Although the government may try to draw bright-line distinctions between the two, the reality is far murkier and typically depends on context. A change in technical protocols or standards can cause information traditionally regarded as metadata to be treated as content, and vice-versa.[4] But the task here is not to define "metadata," nor do *amici* believe it

---

making calls. Instead, it provide [*sic*] a record of phone numbers and the times and length of calls, metadata . . . ."); Gov. Opening Brief at 30, 45-46.

[4] In communications technology, "metadata" is often defined by what it is not: it is not the "content" (or "payload") of a communication, but even this distinction depends on context. For example, a website URL entered by a user could be considered a form of metadata, since it is part of a routing request by the user to receive the contents of the website located at the URL address. Yet, quite obviously, the URL itself conveys information about the contents of the site. Just as dialing the San Francisco Suicide Prevention hotline can reveal information about the caller's conversation, so too can visiting the hotline's online live chat page, http://www.sfsuicide.org/get-help/livechat. For further discussion of the technical nuance required to define metadata, *see* Steven M. Bellovin, *Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the*

practical or useful to do so in a categorical way. Rather, the relevant fact for whether an expectation of privacy exists is that the comprehensive telephone records the government collects—not just the records of a few calls over a few days but *all* of a person's calls over many years—reveals highly personal information about the person and her life.

Under the call records collection program, the "telephony metadata" collected includes (at least[5]) the following information:

> [C]omprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, Internal Mobile station Equipment Identity (IMEI) number, etc.), International Mobile Subscriber Identity (IMSI) number, trunk identifier, telephone calling card numbers, and time and duration of call.

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *1 n.2 (FISA Ct. Aug. 29, 2013) ("BR 13-109"). IMSI and IMEI numbers are unique numbers that

---

§ 215 and § 702 Surveillance Programs 5-7 (July 31, 2013), *available at* https://www.cs.columbia.edu/~smb/papers/PCLOB-statement.pdf.

[5] The government has also now admitted to collecting cell site location data on a test basis at one time under Section 215. *See* Letter from Nat'l Sec. Agency Legislative Affairs Office to Senate Select Committee on Intelligence 2, (Dec. 1, 2010), *available at* http://www.dni.gov/files/documents/1118/CLEANED010.%20RFI%20Response_SSCI%20Gottte...es%201%20December%202010-Sealed.pdf. Additional information may be collected as well.

identify the user or device that is making or receiving a call.[6] In conjunction with originating and terminating telephone numbers, for the vast majority of telephone users, these numbers can be used to identify a specific user and device.[7] A "trunk identifier" provides information about how a call is routed through the phone network, revealing general information about the parties' locations. The other data collected includes the calling card number used (if one is used), and the time and duration of a call.

As explained more fully below, this information reveals deeply personal information about Americans' habits, interests, beliefs, and relationships.

---

[6] *See* Privacy and Civil Liberties Oversight Bd., Report on the Telephone Records Program 26 n. 52 (Jan. 23, 2014) ("PCLOB Report"), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

[7] Although the government does not collect the names of those associated with the telephone numbers, telephone numbers are, themselves, identifying, in the same way that social security numbers are. In any event, the additional step of associating a name with an individual's metadata is trivial. The government, like all Americans, has ready access to public and commercial databases that match telephone numbers to actual names. *See, e.g.*, Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA's Got Your Number* (Dec. 23, 2013), http://webpolicy.org/2013/12/23/metaphone-the-nsas-got-your-number. For the relatively few names that are not publicly accessible, the government also has a number of legal tools, such as criminal subpoenas and National Security Letters, at its disposal to compel production of a phone subscriber's name. *See* 18 U.S.C. §§ 2703, 2709.

A. Telephony Metadata Reveals Sensitive Information, Even in Limited Quantities.

Although the "telephony metadata" obtained by the government may, on its face, appear innocuous, it is anything but. Even at the level of single calls, telephony metadata can uncover private and sensitive information.

A call to a hotline or another type of dedicated, single-purpose phone line provides perhaps the starkest demonstration of this power. An hour-long call at 3 A.M. to a suicide prevention hotline; a thirty-minute call to an alcohol addiction hotline on New Year's Eve; or a fifteen-minute call to a phone-sex service—the "metadata" from those calls, even in the absence of the "content" of the conversation, still reveals information that virtually anyone would consider exceptionally private.[8]

Disclosure of metadata from a handful of calls can yield equally sensitive information about a caller. For example: a person makes a series of calls—first, to an HIV testing service; then, a doctor; then to a loved one; and then, an insurance company. A likely narrative emerges—an individual coping with a new diagnosis

[8] Indeed, metadata about a single call can reveal *more* information than the "content" of the call itself. For example, many wireless telephone companies allow subscribers to donate to charities by sending a text message to a specified "short code," corresponding to the charity. *See* Declaration of Edward W. Felten, *ACLU v. Clapper*, No. 13-cv-03994 (WHP) (S.D.N.Y. Aug. 23, 2013), ECF No. 27 ("Felten Decl."), ¶¶ 43-45. The metadata about these texts reveals that the subscriber has donated to a specific charity or cause, while the content of the message contains at most a donation amount. *Id.* ¶ 45.

of HIV—that is apparent even without examining the content of any communication.

The revelatory nature of even a relatively limited sample of call records is backed up by real world data. Stanford researchers analyzing just a few months of telephony metadata provided by 546 volunteers were able to learn startlingly intimate details. They identified one plausible inference of a subject obtaining an abortion; one subject with a heart condition; one with multiple sclerosis; and one who owned a specific brand of firearm.[9] More generally, a *majority* of the subjects in the study made individual calls that gave rise to "sensitive inferences," such as calls to religious organizations, specific health care providers, political campaigns, and marijuana dispensaries. As the authors of the study explained, "if a person speaks at length with a religious institution, it appears likely that the person is of that faith."[10]

B. In the Aggregate, Telephony Metadata Is Even More Revealing.

Although seemingly counterintuitive, telephony metadata may actually be *more* revealing than the "content" of conversations, especially when collected *en masse*. This is so for two reasons: First, the aggregation of metadata can reveal

[9] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata.

[10] *Id*.

context beyond what is revealed in a single conversation.[11] Second, the structured nature of telephony metadata lends itself more readily to powerful data analysis.

The quantity of telephony metadata collected under the program is vast. *See* BR 13-109, at *1 (noting that the government obtains "a very large volume of each company's call detail records"). The government apparently collects the metadata on a daily basis for all calls originating or terminating in the United States and carried by the nation's largest telecommunication carriers.[12] NSA then retains this data for five years.[13] Thus, even under extraordinarily conservative estimates, the government maintains a database of billions of call records—call records, which in turn, can reveal the details of the most sensitive, intimate, and personal aspects of the lives of millions of Americans.[14]

---

[11] *See* Matt Blaze, *Phew, NSA is Just Collecting Metadata. (You Should Still Worry)*, Wired (June 19, 2013), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again ("Metadata is our *context*. And that can reveal far more about us—both individually and as groups—than the words we speak.").

[12] *See* Siobhan Gorman, *et al.*, *U.S. Collects Vast Data Trove*, Wall St. J. (June 7, 2013), *available at* http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922.

[13] *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* 97 (Dec. 12, 2013) ("President's Review Grp."), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[14] Despite the government's claims that the intrusiveness of the call records program is limited because searches of the call records databases are conducted

Such a large database of telephony metadata can readily reveal extremely sensitive information. Aggregation provides context and information that is not always apparent from the "content" of a communications, such as the insight that people in a relationship call each other regularly, and that, if they stop doing so, the relationship may have ended. *See* Felten Decl. ¶ 49. Aggregated telephony metadata also allows analysts to create "social graphs" that map the network of connections between individuals and social groups, revealing friendships, business relationships, and social and political connections. Using aggregated metadata, an analyst could determine the membership, structure, or participants in organizations and movements like the NAACP, the Tea Party, or Occupy Wall Street, as well as estimate the number of people attending a particular church or political meeting.

The metadata acquired through the government's program is also uniformly structured, allowing it to be easily processed to reveal even more sensitive patterns of conduct of communication. Telephone, IMSI, and IMEI numbers are standardized and expressed in a fixed and predictable format, as are times, dates,

---

only when there is reasonable, articulable suspicion, a single search of the call records database has the capacity to sweep in thousands—if not millions—of Americans' call records. *See* PCLOB Report at 28-29. Although the government has recently modified its search procedures to only use two "hops," rather than three, such searches still yield thousands of responses by a conservative estimate. *Id.* at 29. Moreover, metadata responsive to an NSA search is then placed into the agency's repository or "corporate store," estimated to contain 120 million telephone numbers, and which is not subject to the court-imposed limitations on search. *Id.* at 30-31.

and durations of calls. This standardization and predictability make the data simple to aggregate, store, and analyze using powerful data analysis programs.[15]

Structured data, including telephony metadata, is therefore ideally suited for computational analysis using automated data mining, machine learning, and link-analysis tools. Employing these tools, researchers have been able to mine large pools of metadata, yielding startling observations about personal details, habits, and behaviors. Analysis of telephony metadata alone has shown that "individuals have unique calling patterns, regardless of which telephone they are using;"[16] predicted "whether [a] phone line is used by a business or for personal use;[17] identified callers by social group (workers, commuters, and students) based on their calling patterns,[18] and even estimated the personality traits of individual

[15] By contrast, the content of a given telephone conversation is far less structured. Human speech is not mechanical, and its myriad variations make it more difficult for computers to accurately process. Although voice-recognition software has made significant advances, it is still a difficult, time-consuming, and error-prone process. And, even if the *transcription* process is accurate, the *meaning* of a conversation must still be deciphered, a process that remains notoriously difficult for computers.

[16] Corrina Cortes, *et al*., *Communities of Interest*, AT&T Shannon Research Labs, *available at* http://www.research.att.com/~volinsky/papers/portugal.ps.

[17] Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research, http://bit.ly/153pMcI.

[18] Richard Becker, *et al*., *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, AT&T Labs-Research, http://soc.att.com/ http://soc.att.com/16jmKdz.

subscribers."[19] Felten Decl. ¶ 61. Similarly, the Stanford study of telephony metadata showed that it is possible to automatically identify whether an individual is in a relationship and, if so, with whom, solely based on telephone metadata pattern analysis.[20]

In sum, the metadata collection program operated by the government is a far cry from the limited capabilities of the pen register, used, as in *Smith*, to track a single number for a matter of days. *See* 442 U.S. at 737. Metadata collected about one person over a long period of time—here, the government keeps the information for at least five years—is more revealing than over a short one; and the aggregation of data about many people is yet more revealing, particularly with respect to previously unnoticed connections between individuals.

C. Creating a Trail of Sensitive Metadata Is an Unavoidable Byproduct of Modern Life.

Nor can the collection of telephony metadata be considered in a vacuum. Looking beyond telephone records demonstrates the great risk to privacy in accepting the government's proffered bright line between "content" and "metadata." Metadata is by no means limited to telephone records; it is truly

---

[19] Rodrigo de Oliveira, Alexandros Karatzoglou, Pedro Concejero, Ana Armenta & Nuria Oliver, Towards a Psychographic User Model from Mobile Phone Usage, CHI 2011 Work-in-Progress (May 7–12, 2011), http://bit.ly/1f51mOy.

[20] Mayer & Mutchler, *supra* note 9.

ubiquitous, created through the innumerable and near-continuous digital transactions and interactions attendant to modern life. "Everyone leaves personal digital tracks . . . whenever he or she makes a purchase, takes a trip, uses a bank account, makes a phone call, walks past a security camera, obtains a prescription, sends or receives a package, files income tax forms, applies for a loan, e-mails a friend, sends a fax, rents a video, or engages in just about any other activity."[21]

Because of the ubiquity and diversity of the data generated by individuals, estimates of scale are difficult to generate. By way of example, the *New York Times* reported that under an NSA program, the Agency is equipped to collect 94 different metadata "entity types" for a total of 20 billion "record events" each day,[22] and the types of information created in Internet communications continues to grow.[23] Crucially, nearly all of this metadata is created as a result of an individual's interactions with third parties—including telecommunications and Internet service providers, banks, and retailers—with whom the data normally resides.

---

[21] Nat'l Research Council of the Nat'l Academies of Sci., *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* 3 (2008).

[22] James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times (Sep 28, 2013), *available at* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html.

[23] For example, when the transition to Internet Protocol Version 6 is completed, "web communications will include roughly 200 data fields, in addition to the underlying content." President's Review Grp. at 121.

And, just as aggregated telephony metadata is more revealing than a single call record, so too are aggregated sets of other metadata more revealing than their isolated components.[24]

Location data, created by mobile devices as they connect to cell towers, has been shown to be a particularly rich source for ascertaining personally revealing information. In one study involving location data, researchers developed a model to accurately guess individuals' future movements based on the movements of their friends.[25] Another study presented a predictive model for ethnicity and relationship

[24] A project at MIT Media Lab called Immersion accesses volunteers' email metadata and produces a detailed visualization of their social graph. *See* Immersion, https://immersion.media.mit.edu ("Immersion collects only the metadata (*From, To, Cc* and *Timestamp*) of emails. Immersion does not access the subject or body of any of your emails.") Researchers viewing a volunteer's user patterns can make educated guesses about which people are central to the volunteer's professional, romantic, and social life. *Id*. Metadata from social networks such as Facebook can similarly be used to infer private facts, such as sexual preference. *See* Carter Jernigan and Behram Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, First Monday (Oct. 5, 2009), http://firstmonday.org/article/view/2611/2302; Michael Kosinski, *et al*., *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 Proc. Nat'l. Acad. Sci 5802 (2013), *available at* http://www.pnas.org/content/early/2013/03/06/1218772110.abstract.

[25] Eunjoon Cho, *et al*., *Friendship and Mobility: User Movement In Location-Based Social Networks* (2011), *available at* http://roke.eecs.ucf.edu/Reading/Papers/Friendship%20and%20Mobility%20User%20Movement%20In%20Location-Based%20Social%20Networks.pdf.

status based solely on location.[26] A third found that the correlation of as few as four points in time and place were enough to positively identify nearly all individuals in a location dataset.[27]

As these examples show, any decision about the legal protection afforded telephony metadata will have broad privacy effects, and the ubiquity and revealing nature of these other forms of metadata—many of them creatures of the digital age—cannot be ignored when assessing the government's claim that "metadata" is categorically unprotected by the Fourth Amendment.

II. THE BULK COLLECTION OF TELEPHONE RECORDS VIOLATES INDIVIDUALS' REASONABLE EXPECTATION OF PRIVACY.

More than forty years ago, the Supreme Court noted there is "understandably, a deep-seated uneasiness and apprehension" that government surveillance "will be used to intrude upon cherished privacy of law-abiding citizens." *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div. ("Keith")*, 407 U.S. 297, 312 (1972). As discussed above, the government's collection of

---

[26] Yaniv Altshuler, *et al*., *Incremental Learning with Accuracy Prediction of Social and Individual Properties from Mobile-Phone Data* (2012), *available at* http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6406354&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6406354.

[27] Yves-Alexandre de Montjoye, *et al*., *Unique in the Crowd: The Privacy Bounds of Human Mobility* (2013), *available at* http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html.

telephony metadata provides the government with a rich font of details about Americans' personal lives, details that they customarily and justifiably regard as both private and protected by the Fourth Amendment from warrantless government inspection.

Nevertheless, the government continues to maintain that the constitutional challenge to the program presents an easy case settled long ago, because under the "third-party doctrine," the collection of call records is not a "search" because plaintiffs and the millions of other Americans voluntarily give this information to their telephone companies. *See* Gov. Opening Br. at 45-46 (citing *Smith*, 442 U.S. at 743–44).

But, as the court below recognized, the outcome of this case is not bound by *Smith v. Maryland*, which was decided on starkly different facts. 957 F. Supp. 2d at 31 (remarking that the issue in *Smith* was "a far cry from the issue in this case"). Simply put, bulk collection is different and—as this Court and the Supreme Court have recognized—not governed by the limited reach of *Smith*. To decide this case, the Court must instead determine whether the bulk collection here invades a constitutionally protected privacy interest and therefore constitutes a search under the Fourth Amendment. *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (a search under the Fourth Amendment occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable"); *Katz v. United*

States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Given the especially revealing nature of aggregated telephony metadata, the Court should find that it does.

A. *Smith* Does Not Authorize the Bulk Collection of Revealing Personal Information Such as Telephony Metadata.

When considered in light of the invasiveness of the government's call records collection program and the revealing nature of the data collected, *Smith* cannot bear the weight assigned to it by the government. In *Smith*, the Baltimore police suspected that Smith was making threatening and obscene phone calls to a woman he had robbed days earlier. To confirm their suspicions, they asked Smith's telephone company to install a "pen register" on his line to record the numbers he dialed. After just three days, the pen register confirmed that Smith was the culprit. 442 U.S. at 737. The Supreme Court upheld the warrantless installation of the pen register in Smith's case, but the stakes were small: The pen register was primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls, *id.* at 741; it was in place for only three days; and it was directed at a single criminal suspect, *id.* at 737.

Thus, the question in *Smith* was only whether a specific individual—someone suspected of having committed a serious crime and identified after a targeted investigation without the aid of any electronic surveillance—had a reasonable expectation of privacy in the list of individuals he had called over the

course of three days. Here, by contrast, the question is whether plaintiffs and their fellow Americans have a reasonable expectation of privacy in the mass of telephony metadata they have generated over the period of many years. As the lower court explained, that is a novel question that *Smith* did not address. *Klayman v. Obama*, 957 F. Supp. 2d 1, 31 (D.D.C. 2013).

Saying there is no difference between the primitive pen register in *Smith* and the bulk phone records program is like saying, as the Supreme Court recently observed in the context of cell phone search, "a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley v. California*, 134 S. Ct. 2473, 2488 (2014). The differences between the government's mass telephone records collection and the pen register in *Smith* are stark, including:

- **Scale**: The program collects data for *all or nearly all* Americans, rather than one individual suspected of a serious crime. *Klayman*, 957 F. Supp. 2d. at 33.
- **Duration**: The current program captures years of data, while the pen register in *Smith* captured data for only three days. *Id.* at 32.
- **Changes in telephone use:** Use of the telephone has changed dramatically since 1979, when telephones were largely stationary devices shared among a number of users, with one number per

household or organization. Today, as landline usage dwindles, mobile phones have become personal, not shared, devices that many people carry constantly with them and use dozens, if not hundreds, of times per day. *See id.* at 34-35.

- **Information collected**: The phone records in this case include whether the call was completed, its duration, and other information rather than simply which numbers were being dialed, as in *Smith*. *See id.* at 36 n. 57
- **Individualized suspicion:** The program does not collect information based on individualized suspicion of any sort, much less individualized suspicion of a crime.

The combination of these factors—especially breadth, duration, and advances in technology—allows the government to draw extremely revealing insights based on metadata alone, a result unimaginable when *Smith* was decided and certainly not considered by the Court. *Id.* at 33, 35-36.

Subsequent decisions relying on *Smith* to uphold warrantless surveillance do not approach the bulk phone collection program engaged in by the government. For example, the Ninth Circuit in *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2008), extended *Smith* to the use of a pen register to capture Internet metadata like IP addresses because it involved targeted surveillance of individuals suspected of

criminal activity for discrete periods of time. But the court noted that its holding did not extend to "more intrusive" surveillance methods, or those that would reveal more sensitive "content"-like information. *Forrester*, 512 F.3d at 511.

More broadly, there is widespread judicial recognition that whether a reasonable expectation of privacy exists does not turn simply on whether electronic data is in some sense "disclosed" to a third-party communications service provider, and that the government does not have a free pass to engage in the suspicionless collection of massive data sets that reveal the intimate details of a person's life, as do the many years of phone records here. Even in non-digital contexts, this so-called third-party doctrine has never been an on-off switch for constitutional protections. For instance, the Supreme Court in *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001), found a "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." In *Stoner v. California*, 376 U.S. 483, 489-90 (1964), the court protected a hotel guest against police entry even after finding that he "gives implied or express permission to such persons as maids, janitors or repairmen to enter his room in the performance of their duties." (internal citations and quotations omitted). And in *Chapman v. United States*, 365 U.S. 610, 616 (1961), the Supreme Court held that even though a landlord may enter "to view waste," police intrusion, even with

landlord's permission, is still subject to the Fourth Amendment. *See also Bond v. United States*, 529 U.S. 334, 338–39 (2000) (expectation of privacy in contents of personal luggage in overhead bin on bus); *United States v. Young*, 573 F.3d 711, 716-17 (9th Cir. 2009) (expectation of privacy in hotel room and luggage left in room).

The issue is even more problematic in the twenty-first century in a way that earlier courts could not have foreseen. As Justice Sotomayor wrote in *Jones*, *Smith*'s nearly forty-year-old premise is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing *Smith*, 442 U.S. at 742 and *United States v. Miller*, 425 U.S. 435, 443 (1976)). Other courts have not shied away from distinguishing *Smith* when the government uses more intrusive surveillance techniques or obtains more revealing personal information. For example, a person sending an email "voluntarily discloses" the electronic contents of the email to the email provider so the email may be transmitted and/or stored, just as a person making a phone call "voluntarily discloses" the number she dials so that the call may be completed. Yet the email sender nonetheless retains a reasonable expectation of privacy in the email she has disclosed to her email provider. *United States v. Warshak*, 631 F.3d 266, 286-87 (6th Cir. 2010); *United States v. Cotterman*, 709 F.3d 952, 964 (9th

Cir. 2013 (en banc) (emails "are expected to be kept private and this expectation is one that society is prepared to recognize as reasonable") (internal quotations omitted). And very recently, the Eleventh Circuit found a reasonable expectation of privacy in cell phone location records stored by a cell phone provider. *United States v. Davis*, 754 F.3d 1205, 1216-1217 (11th Cir. 2014) (Sentelle, J.). The bulk collection of telephony metadata here is entirely removed from the limited, targeted surveillance authorized in *Smith*. Instead, decisions like *Davis, Cotterman*, and *Warshak* have found revealing data obtained through "more intrusive" surveillance practices to be constitutionally protected even though the records are held by third parties. *See Forrester*, 512 F.3d at 511.

B. Dragnet Collection of Highly Revealing Information Is a Fourth Amendment "Search."

Even at the time *Smith* was decided, courts recognized that dragnet surveillance of the kind at issue here is constitutionally distinct from the pen register used against the criminal suspect in *Smith* and established that dragnet surveillance invades interests protected by the Fourth Amendment.

Indeed, just four years after *Smith*, the Supreme Court made this difference explicit when it considered the warrantless use of a beeper to track the car of a suspected manufacturer of illicit drugs. *See Knotts*, 460 U.S. at 276. While the Supreme Court held that the defendant lacked a reasonable expectation of privacy in his public movements, it harbored no illusion that *Smith* could extend so far as

to justify—as the defendant had warned—"twenty-four hour surveillance of any citizen of this country." *Id.* at 283 (quotation marks omitted). Instead, noting "reality hardly suggests abuse," the Supreme Court nonetheless reserved the right to consider "dragnet type law enforcement practices" if they eventually occurred in the future. *Id.* at 283-84.

More recently, in *United States v. Maynard*, 615 F.3d at 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012), this Court applied this distinguishing principle from *Knotts* and held that the government's long-term tracking of an individual's movements by means of a GPS device attached to his car amounted to a search for Fourth Amendment purposes. The *Maynard* court specifically rejected the same sort of invitation to broadly apply a narrow precedent that the government advances here. The court explained that although the Supreme Court had previously held in *Knotts* that a defendant lacked a reasonable expectation of privacy in his movements on the public streets when tracked for a short period, this decision *did not* mean that an individual "has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it." 615 F.3d at 557.

In *Maynard*, the distinction lay in the significantly more revealing nature of aggregated location data obtained through prolonged tracking. "[T]he whole of one's movements over the course of a month . . . reveals far more than the

individual movements that it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that . . . may reveal even more." *Id.* at 561–62. This Court recognized the immense power of locational metadata to draw sensitive inferences; just as a sequence of telephony metadata tells a story, "[r]epeated visits to a church, a gym, a bar, or a bookie tell a story not told by a single visit," and "[t]he sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story." *Id.* at 562. When such collection is done not just for one individual but for all or most Americans, as here, this Court's insights in *Maynard* apply with even greater force.[28]

Unanimously affirming *Maynard* in *Jones*, all nine Supreme Court justices agreed with this Court's conclusion that such dragnet surveillance raises unique and novel questions, not controlled by prior precedent. *See Jones*, 132 S. Ct. at 954

[28] In *Davis,* the Eleventh Circuit held that the warrantless collection of cell site location information violated a defendant's reasonable expectation of privacy. 754 F.3d at 1216. Taking note of this Court's concerns about the prolonged tracking at issue in *Maynard*, the court held that it need not even resort to the "mosaic theory." *Id*. at 1215. "[E]ven one point of cell site location data can be within a reasonable expectation of privacy" because "[o]ne's cell phone, unlike an automobile, can accompany its owner anywhere." *Id.* at 1216. Just as with a single phone call, a single piece of cell site metadata can reveal "a person's first [private] visit to a gynecologist, a psychiatrist, a bookie, or a priest." *Id.*

("It may be that achieving [long-term location tracking] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."); *id.* at 964 (Alito, J., concurring); *id.* at 955–56 (Sotomayor, J., concurring). Although the majority in *Jones* decided the case on trespass grounds rather than an expectation of privacy analysis, in two concurring opinions five of the Justices made clear that they would resolve that question as had this Court. Justice Alito concluded that "that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment," *id.* at 964 (Alito, J., concurring), and Justice Sotomayor concurred that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy,'" *id.* at 955 (Sotomayor, J., concurring).

The Supreme Court's recent decision in *Riley v. California* reiterated the principle that it articulated in *Knotts* and that this Court followed in *Maynard*: that old precedent addressing limited invasions of privacy does not control new uses of technology that allow invasions on a categorically different scale. In ruling that the storage capacity of a modern cell phone triggers privacy concerns when searched incident to an arrest, the Court remarked that technology like a smartphone "allows even just one type of information to convey far more than previously possible," noting that thousands of photos on a phone could reconstruct the "sum of an

individual's private life" in a way that just one or two photos found in an arrestee's pocket could not.[29] 134 S. Ct. at 2489. As a result, just because a pre-digital search could have turned up one or two photos, this did not justify searching thousands of photos. *Id*. at 2493 ("The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.") In short, *Riley* makes plain that courts must recognize that earlier Fourth Amendment cases cannot be blindly applied in the digital age, and that "any extension of that reasoning to digital data has to rest on its own bottom" rather than relying on analogies to earlier technology. *Id*. at 2489. Because the privacy intrusion was so great, *Riley* refused to extend two older cases involving police searches of physical items, *Chimel v. California*, 395 U.S. 752 (1969) and *United States v. Robinson*, 414 U.S. 218 (1973), to the data on a cell phone, and instead concluded police could not search a cell phone's data incident to arrest. *Riley*, 134 S. Ct. at 2485.[30]

---

[29] Because the parties agreed there was a Fourth Amendment "search," *Riley* specifically noted it was not considering "whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." 134 S. Ct. at 2489 n. 1.

[30] A similar principle can be derived from the Ninth Circuit's *en banc* decision in *Cotterman*, which held that that the forensic examination of a computer triggered greater privacy concerns than a cursory look at an electronic device. 709 F.3d at 968. The Ninth Circuit explained "technology matters" in the Fourth Amendment calculus. *Id.* at 965. As a result, an earlier Supreme Court case authorizing a suspicionless comprehensive border search of a car and its gas tank, *United States*

Thus, the issue presented in this case must be resolved through the familiar inquiry described by Justice Harlan in *Katz*—that is, by asking whether individuals have a reasonable expectation of privacy in the information the government seeks. *Smith* may be relevant to that inquiry, but so too are the decisions—particularly *Knotts*, *Maynard*, *Jones*, *Davis*, and *Riley*—that come after it and which recognize the invasiveness of a specific piece of technology or surveillance technique matters in the constitutional analysis.

Here, what *Knotts*, *Riley*, *Maynard* and the *Jones* concurrences observed of other techniques is equally true of the bulk collection of Americans' call records. As noted earlier and by the district court below, the bulk collection of telephony metadata allows the government to obtain private information in which individuals have a reasonable expectation of privacy. As the district court wrote, "Admittedly, what metadata *is* has not changed over time. . . . But the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly,* what that information can tell the Government about people's lives. . . . [T]hese trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable." 957 F. Supp. 2d at 35–36. As discussed above, a comprehensive record of Americans' telephonic

---

v. Flores-Montano, 541 U.S. 149, 152 (2004), did not authorize a suspicionless comprehensive search of the digital contents of an electronic device because the privacy intrusions were not the same even if the legal doctrine—the border search exception to the warrant requirement—was. *Cotterman*, 709 F.3d at 967.

associations can reveal a wealth of detail about familial, political, professional, religious, and intimate relationships—the same kind of information that could traditionally be obtained only by examining the contents of communications. *See* Felten Decl. ¶¶ 38–64; *see also* PCLOB Report 156–58.

These features of the call-records program—features that the government has never disputed—dictate that a Fourth Amendment search takes place when the government collects telephony metadata belonging to the plaintiffs and millions of other Americans. The program is akin to the "reviled" general warrants "which allowed British officers to rummage through homes in an unrestrained search" and provided both fuel for the American revolution and the primary motivation for adoption of the Fourth Amendment. *Riley*, 134 S. Ct. at 2494. This Court should recognize the serious invasion of privacy worked by the program and hold that it violates the Fourth Amendment.

As described above, it is not *just* metadata. The massive quantity of data the government has collected provides a window into the thoughts, beliefs, traits, habits, and associations of millions of Americans. The Court should reject any contrary suggestion. Given the detailed portrait that can be drawn from metadata alone—and given the especially revealing nature of large quantities of metadata—the collection of this sensitive information receives the highest protection of the Fourth Amendment.

CONCLUSION

For the reasons given above, the district court's order granting a preliminary injunction in No. 13-cv-00881-RJL should be affirmed.

Dated: August 20, 2014

Respectfully submitted,

/s/ Mark Rumold
Mark Rumold
Andrew Crocker
Hanni Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
mark@eff.org
Counsel for Amici Curiae

Of Counsel:
Alex Abdo
Patrick Toomey
Jameel Jaffer
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
aabdo@aclu.org

Arthur B. Spitzer
AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL
4301 Connecticut Avenue, N.W., Suite 434
Washington, DC 20008
Phone: (202) 457-0800
artspitzer@aclu-nca.org

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 28.1(e)(2) or 32(a)(7)(B) because:

   [X] this brief contains 6,885 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), or

   [ ] this brief uses a monospaced typeface and contains [state the number of] lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   [X] this brief has been prepared in a proportionally spaced typeface using Microsoft Word for Mac 2011 in 14pt Times New Roman; or

   [ ] this brief has been prepared in a monospaced typeface using [state name and version of word processing program] with [state number of characters per inch and name of type style].

Dated: August 20, 2014

Respectfully submitted,

/s/ Mark Rumold
Mark Rumold
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

CERTIFICATE OF FILING AND SERVICE

I HEREBY CERTIFY that on this 20th day of August, 2014, I filed a true and correct copy of foregoing brief with the Clerk of the United States Court of Appeals for the District of Columbia Circuit. All participants in the case are registered CM/ECF users and will be served by the appellate CM/ECF system. I further certify that I will cause eight (8) paper copies of this brief to be filed with the Court.

Dated: August 20, 2014

Respectfully submitted,

/s/ Mark Rumold
Mark Rumold
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae