No. 14-35555

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ANNA SMITH,

Plaintiff-Appellant,

v.

BARACK OBAMA, *et al.*,

Defendant-Appellees.

On Appeal from the United States District Court
for the District of Idaho, Boise; Case No. 12:13-cv-00257-BLW
The Honorable B. Lynn Winmill, Chief District Judge

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-THREE TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF APPELLANT

Marc Rotenberg
Counsel of Record
Alan Butler
Julia Horwitz
Jeramie Scott
Electronic Privacy Information Center
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

September 9, 2014

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTEREST OF THE AMICI[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other Constitutional values.

EPIC routinely participates as *amicus curiae* before federal and state courts in cases concerning the protection of privacy. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013); *Florida v. Harris*, 133 S. Ct. 1050 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012); *Herring v. United States,* 555 U.S. 135 (2009); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada*, *Humboldt Cnty.,* 542 U.S. 177 (2004); *State v. Earls*, 214 N.J. 564 (2013); *Commonwealth v. Connolly*, 454 Mass. 808 (2009).

EPIC has a particular interest in the NSA surveillance program as the organization has testified before Congress on the need to limit the scope of the agency's surveillance activities and brought the first challenge to the NSA telephone record collection program to the Supreme Court. *In re EPIC*, 134 S. Ct. 638 (2013).

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

Several members of the EPIC Advisory Board are expert in the matter currently before this Court and have written extensively on the legal, technical and policy issues arising from the NSA's domestic surveillance activities. *See*, *e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J. L. & Pub. Pol'y 759 (2013); Bruce Schneier, *Metadata Equals Surveillance*, Schneier on Security (Sept. 23, 2013).

The EPIC amicus brief is joined by 33 technical experts and legal scholars:

EPIC Technical Experts and Legal Scholars

Alessandro Acquisti, Professor, Heinz College, Carnegie Mellon University

James Bamford, Author and Journalist

Ann Bartow, Professor of Law, Pace Law School

Colin J. Bennett, Professor, University of Victoria

Francesca Bignami, Professor of Law, George Washington University School of Law

Christine L. Borgman, Professor & Presidential Chair in Information Studies, University of California Los Angeles

danah boyd, Founder, Data & Society Research Institute

Julie E. Cohen, Professor of Law, Georgetown University Law Center

Danielle Keats Citron, Lois K. Macht Research Professor of Law, University of Maryland School of Law

Cynthina Dwork, Distinguished Scientist, Microsoft

Simon Davies, Project Director, London School of Economics

Laura K. Donohue, Professor of Law, Director of the Center for National Security and the Law, Georgetown University Law Center

David Farber, Distinguished Career Professor of Computer Science and Public Policy, School of Computer Science, Carnegie Mellon University

Addison Fischer, Former Owner, RSA Data Security; Co-Founder, Verisign

David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Deborah Hurley, Chair, EPIC Board of Directors

Kristina Irion, Institute for Information Law, University of Amsterdam

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Ripple Labs Inc.

Harry Lewis, Gordon McKay Professor of Computer Science, School of Engineering and Applied Science, Harvard University

Anna Lysyanskaya, Professor of Computer Science, Brown University

Gary T. Marx, Professor Emeritus, Massachusetts Institute of Technology

Dr. Pablo Molina, Adjunct Professor, Georgetown University

Helen Nissenbaum, Professor, Media, Culture and Communications, New York University

Frank Pasquale, Professor of Law, University of Maryland Carey School of Law

Dr. Deborah C. Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Barbara Simons, IBM Research (retired)

Frank Tuerkheimer, Professor of Law, University of Wisconsin Law School

Sherry Turkle, Abby Rockefeller Mauzé Professor, Massachusetts Institute of Technology

Edward Viltz, President, Internet Collaboration Coalition

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

This case presents a critical Constitutional question: whether the collection of all domestic telephone records of American telephone customers violates a reasonable expectation of privacy. The Supreme Court has never considered government surveillance activity of this scope; current case law relies on an opinion from an era before e-mail, cell phones, and mobile apps, when most metadata was not available to the government because it was never created. Modern communications technology generates a constant stream of detailed information about our private lives, raising concerns about data breaches, identity theft, and the wrongful disclosure of personal information. Legal scholars and technical experts affiliated with EPIC believe that changes in technology and the Supreme Court's recent decision in *Riley v. California* favor a new legal rule that recognizes the privacy interest inherent in modern communications records.

ARGUMENT

The ongoing collection of Americans' telephone call records by the National Security Agency is an unprecedented invasion of privacy that contravenes the core purpose of the Fourth Amendment: to limit the government's ability to search private records without individualized suspicion and the oversight of a neutral magistrate.

The decision of the lower court that the NSA's routine collection of all telephone call records of all telephone customers does not constitute a Fourth Amendment "search" relies on an opinion from the 1970s in which the police monitored calls from a single phone line following the suspicious activity of an identified suspect. *Smith v. Maryland*, 442 U.S. 735 (1979).

Reliance on *Smith v. Maryland* is untenable today for three reasons: (1) communications systems have changed dramatically since the era of the rotary dial phone; (2) the vast amount of metadata generated today was unavailable when *Smith* was decided; and (3) the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), recognized that the privacy interests of phone users today are far greater than the interests the Court considered when phones were tethered to desks, email was for computer geeks, and no one could take a picture by holding up a telephone receiver.

I. The Modern Communications System is Entirely Unlike the Telephone Network of the 1970s

The analog telephone network of the 1970s was entirely unlike the modern digital network that today offers a vast range of voice, data, and messaging services and simultaneously records every transaction that occurs. Telephone service was provided as a public utility, local calls were not individually billed, and there was no opportunity to engage in the massive data mining or network analysis that occurs today. The telephone system did not generate the transactional data that

is a routine part of SS7, the current network technology. So much has changed since the era of the rotary phone that Chief Justice Roberts in the recent unanimous opinion for the Court remarked that we are so attached to our smartphones today that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley* 134 S. Ct. at 2484.

A. In the Analog Era Little Phone Data was Generated

Prior to the introduction of the earliest electronic switching systems in the 1960s and 70s, most telephone calls in the United States were processed by analog switches that had limited accounting and billing capabilities. Most of these analog switches relied on "Automated Message Accounting" systems, which were introduced in the Bell System in 1948 and recorded customer data on perforated paper tapes (earlier systems relied on handwritten notes from telephone operators). G.V. King, *Centralized Automatic Message Accounting System*, 33-6 Bell Sys. Tech. J. 1331, 1332 (1954). These analog accounting systems were designed to handle three different types of calls: flat-rate local calls, message rate calls, and long distance toll calls. *Your Phone Dial Computes Your Bill*, Popular Sci., Feb. 1949, at 135-36. Most local calls were billed on a flat-rate monthly basis, and automated accounting equipment was not used to record any details of these calls. King, *Centralized Automatic Message Accounting System* at 1333. For calls billed on a message rate basis, the accounting system would record a two-line entry

containing "the calling office code and telephone number, the billing index and the trunk identity" along with the duration of the call. *Id*. at 1339. The more extensive four-line entries also contained "the called office code and telephone number," but were only used for detail-billed toll calls and special bulk billed calls that required additional records. *Id*. In situations where a toll call could not be completed by a switch capable of automated message accounting, customers had to be connected via an operator who would manually record the details of the call. *Id*. at 1334-35.

As the automated message accounting system was deployed throughout the United States beginning in the 1950s, it was necessary to centralize the accounting function due to the high cost of the infrastructure relative to the volume of toll calls at many of the smaller local telephone offices. King, *Centralized Automatic Message Accounting System* at 1333; *see also* Phil Lapsley, *Exploding The Phone – Extras* (2013).[2] The automated message accounting system also evolved with the development of "automatic number identification" technology, which was deployed to ensure billing accuracy throughout the Bell System by 1961. *See* Robert J. Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 35 (2003). During the 1950s and '60s, the Bell System continued to install and use centralized automatic message accounting systems, *see* Lapsley, while Bell Laboratories conducted research into new electronic switching systems. Robert J.

[2] *Available at* http://explodingthephone.com/extras/ama.php.

Chapuis & Amos E. Joel, *100 Years of Telephone Switching, Part 2*, at 48-56 (2003). The integration of digital computing technology into the telecommunications industry was ongoing throughout the 1970s, and the evolution of telecommunications services was rapid. *See id*. at 114-115. The first electronic switching system, No. 1 ESS, developed by Western Electric and Bell Laboratories was put into operation in Succasunna, New Jersey in 1965, and each of the 24 Regional Bell Operating Companies had installed at least one ESS by 1967. *Id*. at 158. These electronic switching systems began using magnetic tape drives to store call detail information in the 1970s, but memory was limited and storage of call details was necessarily temporary. *See id*. at 345.

Thus, in the period leading up to the Court's decision in *Smith v. Maryland*, there was no way for the government to routinely obtain call detail information for all calls placed in the United States. Most of the call records, other than certain long distance billing records, simply did not exist. Local call details were ephemeral because most customers paid a flat monthly telephone rate, and did not receive an itemized bill. Robert G. Harris, *State Regulatory Policies and the Telecommunications/Information Infrastructure*, The Changing Nature of Telecommunications/Information Infrastructure (Computer Sci. & Telecomm. Bd. and Nat'l Research Council eds., 1995).

Even after the development of advanced electronic switching technologies, telephone companies had little incentive to store transactional data. By the mid-1970s, magnetic tape backup storage was integrated into the most advanced electronic switches. C.F. Ault, J.H. Brewster, T.S. Greenwood, R.E. Haglund, W.A. Read, & M.W. Rolund, *1A Processor: Memory Systems*, 56-2 Bell Sys. Tech. J. 181, 201 (1977). But there was little space to store phone records as bandwidth had to be preserved for other functions. The shift to "common channel" signaling in 1976 illustrates the technological limitations of previous signaling systems. In a common channel signaling system, separate telephonic channels were required in order to set up a phone call. Harry G. Perros, *Connection-Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks* 296 (2005). These were the signaling channel, which carries call information (such as the destination telephone number) and the bearer channel, which carries the voices. *Id*. In the early 1976, the United States implemented its first "common channel" telephonic signaling system. *Id*.

Previously, telephones had relied on a "channel-associating" system for connecting phone calls. Under the "channel-associating" system, all of the information needed to set up a call (*i.e.*, both voice and call data) was sent over the same channel. "In common-channel signaling, the call information was sent between switches over a channel that was dedicated only to signaling; that is, all

signals had the same channel in common with each other. In the 1970s, the Bell System introduced the CCIS system, which was a variant of CCITT SS6." Martin B. H. Weiss, *Communications Standards*, 4 The Froelich/Kent Encyclopedia of Telecommunications 72 (1992). This meant that the already-limited bandwidth provided for a phone call had to be shared between signal links and bearer links, resulting in lower available bandwidth for the voice information. Matthew Stafford, *Signaling and Switching for Packet Telephony* 56 (2004).

Under the early "common channel" system, called Signaling System 6 or CCIS 6 (after the international standards-setting body that developed SS6), bearer channels and signaling channels were split. Stephen Gorove, Major Milton Smith, Ram Jakhu, Robert R. Bruce, et. al., *Developments in the International Law of Telecommunications Strategic Issues for A Global Telecommunications Market*, 83 Am. Soc'y Int'l L. Proc. 385, 398 (1989). All signaling information occupied one channel, allowing all other channels to become bearer channels. John G. van Bosse & Fabrizio U. Devetak, *Signaling in Telecommunication Networks* 75 (2nd ed. 2007). Bell Laboratories, the company that installed the SS6 in the United States, envisioned many possibilities for common channel signaling, but they could not have predicted the subsequent explosion in advanced telecommunications services that was enabled by future common channel systems. And as the

telecommunications network expanded to provide advanced services, it also began to generate and store an enormous amount of user data.

B. New Consumer Privacy Safeguards Were Established As Caller Identified Data Was Generated

The development of advanced common channel signaling techniques continued in the 1980s and culminated in the development and implementation of Signaling System 7, which was first adopted as a worldwide standard by *International Telegraph and Telephone Consultative Committee* (CCITT) in 1980 and later implemented in the U.S. and other countries. Anu A. Gokhale, *Introduction to Telecommunications* 141 (2nd ed. 2005). "MCI (now part of WorldCom) first implemented SS7 in its network in April 1988 in Los Angeles and Philadelphia." Annabel Z. Dodd, *The Essential Guide to Telecommunications* 219 (3d ed. 2002). Implementation of the SS7 Protocol enabled the development and use of new enhanced services based on the "Intelligent Network" model. *See generally* John Anderson, *Intelligent Networks: Principles and Applications* (2002). These new features created opportunities for businesses to offer new advanced telecommunications services, including, eventually, Internet services, but they also exposed consumers to new privacy risks. And as a result of opposition to new privacy-invasive features, the Federal Communications Commission adopted standards to enable greater user privacy.

One new service in particular, Calling Name Delivery (now known as Caller-ID), caught the immediate attention of consumers, privacy advocates, legislators, regulators, and courts. *See Caller-ID Technology: Hearing on S. 2030 Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary*, 101st Cong. (1990); David B. Hack, Cong. Research Serv., IB 90085, *Caller I.D. and Automatic Telephone Number Identification* (1991). Caller ID allowed telephone companies to disclose to customers "the number of the phone from which an incoming call was placed." John Burgess, *Privacy Issues Pervade Plans For 'Caller ID' Phone Service*, Wash. Post, Dec. 5, 1989, at B1. This new service faced intense backlash because customers wanted to control the disclosure of their telephone numbers and did not want unlisted numbers to be shared. There was also concern that undercover police officers and at-risk individuals, such as women in shelters trying to reach family members, would be discouraged from using phone services. *Id*. The service was also controversial because it allowed marketing firms and other companies to monetize caller records. *See* Mitch Betts, *Firms Seek Their Magic Number Through ISDN*, Computerworld, Feb. 5, 1990, at 67.

As phone providers began to offer Caller ID service, consumers brought legal action to prevent the disclosure of their personal information. In Pennsylvania, users brought a complaint against the Public Utility Commission, which suspended Caller ID on March 31, 1989. *Barasch v. Bell Telephone Co. of*

Pa., 605 A.2d 1198 (Pa. 1992). The Pennsylvania Supreme Court subsequently held that the Caller ID service violated the state's wiretap law because it operated without consent of the telephone users. *Id*. at 1203. The Federal Communications Commission also issued a Final Rule requiring providers of Caller ID services to enable a per-call blocking feature to allow for caller anonymity, but also pre-empted all state law restrictions on the provision of Caller ID services. *See People of the State of Cal. v. FCC*, 75 F.3d 1350, 1357-58 (9th Cir. 1996).

Response by users, lawmakers, and regulators to privacy issues arising from the implementation of SS7 and services such as Caller ID showed that as the amount of transactional information about users' communications increased, new privacy safeguards were necessary to preserve user anonymity and autonomy. But the collection of user data has become even more widespread over the last two decades and Fourth Amendment jurisprudence has failed to reflect the expectation of consumers that their personal phone records will not be routinely collected by the government.

C. Today a Vast Amount of Data is Generated by Phone Companies

In the modern network, so much data is generated about user activities that the privacy interest in non-content data is often greater than the privacy interest in the content of communications. It is the transactional data that allows data mining,

network analysis, link analysis, and event sequencing, analytic techniques that are simply not available with solely the content of communications.

The FISA Court has defined "telephony metadata" as "comprehensive communications routing information, including *but not limited to"*

- Session identifying information
    - Originating telephone number
    - Terminating telephone number
    - International Mobile Subscriber Identity (IMSI) number
    - International Mobile station Equipment Identity (IMEI) number
- Trunk identifier
- Telephone calling card numbers
- Time of call
- Duration of call

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [REDACTED], Br. No. 14-67 at *3 n.2 (FISC Mar. 28, 2014).[3]

The NSA's telephony metadata extend beyond these categories of information. As the FISC explained, "NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata." *Id*. at *12 n.15. So, for example, an NSA analyst could use publicly

[3] *Available at* http://www.dni.gov/files/documents/0627/BR_14-67_Primary_Order.pdf.

available information including "tools such as reverse telephone directories, public search engines and other NSA databases" to identify the phone users. *See* Dana Priest, *Piercing the Confusion Around NSA's Phone Surveillance Program*, Wash. Post (Aug. 8, 2013).[4]

Telephony metadata can be used to identify a person making a call, a person receiving a call, a sequence of communications between people, the participation of others, family relations, business relations, medical conditions, political affiliations, and religious belief. An individual cell phone subscriber may be followed through the International Mobile Subscriber Identity ("IMSI") number, which is unique for every subscriber. Gary Mullett, *Wireless Telecommunications Systems and Networks* 101-102 (2006). This 15-digit number includes a three-digit country code and three-digit mobile network code. *Id*. The IMSI also contains a unique subscriber number assigned by a user's mobile carrier. *Id*. The IMSI is stored in the phone's Subscriber Identity Module ("SIM") card. *Id*. A SIM card is a component of a cell phone that contains essential information about the subscriber. Nat'l Inst. of Stds & Tech., *Guidelines on Cell Phone Forensics*, Special Pub. No. 800-101, at 7 (May 2007).[5] SIM cards are removable and may be used in different

[4] *Available at* http://www.washingtonpost.com/world/national-security/piercing-the-confusion-around-nsas-phone-surveillance-program/2013/08/08/bdece566-fbc4-11e2-9bde-7ddaa186b751_story.html.

[5] *Available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf (A SIM card authenticates the mobile device user to the mobile network

mobile devices. Moving a SIM card to another device transfers a subscriber's IMSI number and other information stored on the SIM. *Id*.

A particular mobile device can also be tracked through the International Mobile Equipment Identity ("IMEI"). Mullett, *supra*, at 102. The IMEI is a 15-digit number that identifies the cell phone's manufacturer, model, and country of approval. NIST at 38. The IMEI is stored directly on the cell phone. *Id*. at 38. Thus, unlike the IMSI, the IMEI remains on the phone, even if the user moves the SIM card to another device.

Mobile carriers maintain IMSI and IMEI numbers with their subscriber records. *Id*. at 53. Subscriber records also typically include information such as the customer's name and address, telephone number, alternate contact information, and credit card numbers. *Id*. at 53. Thus, an IMSI or IMEI can provide access to sensitive personal information about a particular subscriber. Some users might take steps to make it more difficult to link an IMSI or IMEI to their account. For example, an individuals use prepaid cell phones, which be purchased anonymously over the counter. But, as of February 2013, only 28 percent of all mobile customers used prepaid phones. Alina Tugend, *Cellphone Service Without Signing on the Dotted Line*, N.Y. Times, Feb. 9, 2013, at B5. Moreover, even prepaid customers may provide personal information such as credit card numbers used to purchase

---

and can also stores a user's personal information including "phonebook entries, text messages, last numbers dialed (LND) and service-related information.")

additional airtime or email addresses to receive notifications. NIST, *Guidelines on Cell Phone Forensics* at 53. For the vast majority of cell phone users, IMSI and IMEI numbers can be easily connected to their individual subscriber records. *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary*, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.)

To accurately bill a subscriber, mobile carriers record the time and duration of a call. NIST, *Guidelines on Cell Phone Forensics* at 52. Carriers also record location data by logging a call's trunk identifier. A trunk identifier reveals the route through a network that a phone call takes. Verizon, *Glossary of Telecom Terms* (2012) (last viewed Sept. 4, 2014);[6] Hearing *on Continued Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary*, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.). Thus, a trunk identifier can reveal the location of a phone user based on how their call was routed.

Mobile carriers also maintain cell site location information ("CSLI") records for every mobile phone, which can be used to identify the precise location from which each call was made. Although the NSA does not currently collect cell site location information as part of the telephony metadata program, it has admitted

[6] http://www22.verizon.com/wholesale/glossary/Glossary-of-Telecom-Terms-t.html.

to collecting cell location information in the past to test its future capabilities. Ellen Nakashima, *NSA Had Test Project to Collect Data on Americans' Cellphone Locations, Director Says*, Wash. Post (Oct. 2, 2013).[7] Cell site location information includes a record of the tower and tower-sector that a phone is connected to at a particular time (typically when a call is placed). *See* Supplemental Brief of EPIC at 10-14, *State v. Earls*, 214 N.J. 564 (2013). Depending on the range of the cell tower, CSLI can be used to locate a device in a neighborhood or on a particular block, or it can be used to pinpoint a device in a specific building or room. *Id*.

In addition to standard telephony metadata, Verizon and other phone companies also collect a wide range of other data about users. Verizon may collect from its customers information "such as call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information and identifiers, service options you choose, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, FIOS TV viewership, and other similar information." Verizon, *Privacy Policy* (2014).[8] And users maintain strong privacy interests in this data as well. The Federal Communications Commission recently fined Verizon $7.4 Million for failing to provide users with an opt-out prior to using their personal

[7] *Available at* http://www.washingtonpost.com/world/national-security/nsa-had-test-project-to-collect-data-on-americans-cellphone-locations-director-says/2013/10/02/65076278-2b71-11e3-8ade-a1f23cda135e_story.html.
[8] *Available at* http://www.verizon.com/about/privacy/policy/.

information for marketing campaigns. 33 FCC Daily Dig. 166 (FCC Sept. 3, 2014).[9]

II. Communications Metadata Reveals Sensitive Personal Information

The metadata generated today by the telephone network can be analyzed and used to determine intimate details of a user's life including that person's interests, activities, beliefs, and affiliations. Telephony metadata can also reveal associations and personal relations. These large data sets involving millions of records can reveal a very precise picture of private activities.

A. Metadata Reveals Our Social Interactions and Private Associations

Through current data analysis techniques, metadata exposes our social interactions and private associations. Metadata is created by almost every aspect of our daily lives, and the data is held by many organizations. Nat'l Research Council of the Nat'l Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* 32-33 (2008). Our personal "behavior, communications, and relationships" are now routinely recorded. *Id.* And widely available tools can now be used to examine and analyze that data to reveal private information about our actions and associations.

Using metadata, researchers have uncovered private facts about individuals. For example, researchers at AT&T labs have used telephone metadata to predict

[9] Agency documents are available at http://www.fcc.gov/document/verizon-pay-74m-settle-privacy-investigation.

whether a human or a fax machine is making a call,[10] whether a phone line is used for business or personal purposes,[11] what social group a caller belongs to,[12] and to approximate the personality traits of specific subscribers.[13] Analysis of large metadata sets equivalent to those created by the NSA can reveal even more personal information including the identities of our friends and associates, the identities of our loved ones, and even our political, religious, or social affiliations.

In a recent study, Stanford researchers tested the sensitivity of metadata by analyzing the telephone records of several hundred volunteers. *See* Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014).[14] The study gathered a few months of phone activity from 546 participants via an app voluntarily installed on Android smartphones. *Id.* Analysis of this phone data revealed a number of patterns characteristic of very sensitive activities. For example, one participant repeatedly called a specialty firearm store that focuses on semiautomatic rifles and had a lengthy conversation with the customer service

[10] Haim Kaplan, Maria Strauss & Mario Szegedy, *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, 10 Proc. ACM-SIAM Symp. Discrete Algorithms (1999).
[11] Corinna Cortes & Daryl Pregibon, *Giga-mining*, Proc. KDD, New York (1998).
[12] Richard A. Becker, Ramón Cáceres, Karrie Hanson, Ji Meng Loh, Simon Urbanek, Alexander Varshavsky, & Chris Volinsky, *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, 1st Workshop on Pervasive Urban Applications (2011).
[13] Rodrigo de Oliveria, *et. al*, *Towards a Psychographic User Model form Mobile Phone Usage*, Proc. CHI 11' EA Hum. Factors Comp. Sys. (2011)(.
[14] http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

department of an automatic rifle producing firearm manufacturer. *Id.* Another participant "contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop,"[15] all within three weeks. *Id.* Another participant who had a long call with her sister, subsequently called the local Planned Parenthood several times within two days. *Id.* Additional calls were made two weeks later with a final one occurring one month later. The Stanford researchers were also able to infer specific medical conditions (e.g. multiple sclerosis) from the call patterns they observed. *Id.*

All metadata can be used to make inferences about our daily activities, but location data is particularly sensitive since it can uniquely identify individuals, reconstruct a person's movements across space and time, predict future movements, and determine social interactions and private associations. MIT researchers studied a little over a years worth of the mobile phone datasets of roughly 1.5 million users. The MIT researchers found that "four spatio-temporal points are enough to uniquely identify 95% of the individuals." Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Sci. Rep. 3 (2013). Researchers have also studied location data of cell phone users and their acquaintances to accurately predict an individual's future movements. Manlino De

[15] Store that sells tobacco paraphernalia and is often associated with marijuana use.

Domenico, Antonio Lima, & Mirco Musolesi, *Interdependence and Predictability of Human Mobility and Social Interactions*, Pervasive and Mobile Computing 9.6 (2013). Given a large enough data set, analysts can predict an individual's location not only in the immediate future, but even months and years ahead of time. Adam Sadilek & John Krumm, *Far Out: Predicting Long-Term Human Mobility*, 26 Proc. AAAI Conf. Artificial Intelligence (2012). The company Sense Networks "builds proprietary mobile user profiles which incorporate over 1,000 behavioral attributes that are extracted from location data." Sense Networks, *About the Company* (2013).[16]

It was recently revealed that the NSA uses location data collected under a different legal authority to predict the locations of military targets as well as individuals who may come into contact with those targets in the future, and to identify new targets based on patterns of behavior. *See* Ashkan Soltani & Barton Gellman, *New Documents Show How the NSA Infers Relationships Based on Mobile Location Data*, Wash. Post (Dec. 10, 2013).

B. Even Individual Call Records Can Reveal Sensitive Private Facts About Cell Phone Users

The use of certain phone numbers will necessarily reveal sensitive personal information: suicide hotlines, sexual abuse hotlines, gambling or drug addiction hotlines, and domestic abuse hotlines. Without the promise of privacy, many

[16] https://www.sensenetworks.com/company/about-the-company/.

individuals would not be willing to seek the support that they need. Similarly, calls to a physician's office, a gun store, a psychiatrist, a pharmacy, a medical marijuana dispensary, a church, or an abortion clinic would all reveal information about the caller's private activities. Many charities and political groups also now accept donations via text message, so a record of a message sent to one number could reveal the users political affiliation.

In one study, researchers were able to infer from single call records the users: religious affiliation, medical conditions, gun ownership, and political views among other sensitive and private information. *See* Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014). In checking the precision of the inference of religious affiliation, the Stanford researchers were 73% accurate in their assumption "that a person's most-called religion is their own religion." *Id.* Call to health care providers are particularly revealing and 57% of the participants called a health services number. *Id.* Many of the health service phone numbers were associated with specific services. For example, 8% of the participants called a health service provider specializing in mental health and family services, 6% called sexual and reproductive health service providers, and another 1% called a substance abuse number. *Id.*

C. The Government's Analysis of the Phone Metadata Is Specifically Designed to Uncover The Private Associations of Users

The NSA uses computer algorithms to create detailed social graphs through a process known as "contact chaining." *See Documents on N.S.A. Efforts to Diagram Social Networks of U.S. Citizens*, N.Y. Times (Sept. 28, 2013) (showing an internal NSA memo on new "contact chaining" procedures from 2011).[17] The NSA has described contact chaining as "the process of building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities (people, organizations, etc) and their associates from the communications sent or received by targets." Office of the Inspector Gen., Nat'l Sec. Agency, Cent. Sec. Serv., *Working Draft* ST-09-0002 (Mar. 24, 2009) (*discussing a proposed amendment to Department of Defense procedures for contact chaining*).

NSA analysts conduct this contact chaining procedure beginning with a target or "seed" number and extending through all "second and third tier contacts of the identifier." *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 3 (Aug. 9, 2013).[18] Each layer of analysis is referred to as a "hop." The first "hop" includes the numbers that directly contact the target; the second "hop" includes the numbers that directly

[17] *Available at* http://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html?_r=0.
[18] *Available at* https://www.documentcloud.org/documents/750211-administiation-white-paper-section-215.html, http://perma.cc/V7VM-5MAU.

contact first hop numbers; and the third "hop" are those numbers that directly contact the second hop numbers. *Id*. at 3-4. The number of phone records analyzed grows exponentially as the number of hops increases.

The NSA has emphasized that the number of "seed" numbers queried is low, but this ignores the broad impact of the contact chaining process. For example, in 2012, the NSA queried 288 phone numbers (known as "seeds"). The contact chaining algorithms the NSA uses, though, implicate a much larger set of phone numbers. A three-hop analysis would yield 2.5 million numbers if each person contacted 40 unique people. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop* n.3 (Dec. 9, 2013).[19] The NSA stores telephony metadata collected under this program for five years. The social graphing of the past five years of a persons phone number will produce a very detailed and intimate picture of his or her life.

III. The Supreme Court's Holding in *Smith v. Maryland* Is Not Applicable to Modern Metadata After *Riley v. California*

The Supreme Court recently addressed Fourth Amendment protections for phone data in the modern age in *Riley v. California*, 134 S. Ct. 2473 (2014). In *Riley,* the Court considered whether officers could search an individual's cell phone without a warrant, incident to a lawful arrest. The Court ruled unanimously that such searches of modern cell phones were unreasonable: the strong privacy

[19] *Available at* http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/.

interest in the protection of digital records, the qualitatively different nature of modern cell phone data, and the pervasive use of modern mobile devices required a warrant prior to the search. This holding has broad implications, especially for any case involving the collection of digital files and metadata.

In this case, the lower court held that the challenge to the NSA Metadata program must be dismissed because the decision in *Smith v. Maryland*, 442 U.S. 735 (1979), "constrains" the ability of the court to find a reasonable expectation of privacy in telephone call detail records.[20] But the Supreme Court's holding in *Riley* raises substantial questions about the continued relevance of *Smith*.

The Court in *Riley* was concerned not only with the disclosure of photos and other application data, but also with police access to non-content information generated by mobile phones. The Court emphasized that "[d]ata on a cell phone can also reveal where a person has been," and that location information "reflects a wealth of detail about" certain "family, political, professional, religious, and sexual associations." *Riley* 134 S. Ct. at 2490 (citing *United States v. Jones*, 132 U.S. 945, 955 (2012) (Sotomayor, J., concurring)). These are the same considerations now before this Court. The Supreme Court in *Riley* also observed that "call logs typically contain more than just phone numbers" and are thus more sensitive than traditional pen register data. *Id*. at 2493. Moreover, the Court determined that cell

[20] *Smith v. Obama*, ___ F.Supp.2d ___, No. 2:13-cv-00257-BLW, slip op. at 8 (D. Idaho June 3, 2014).

phone data was both quantitatively and qualitatively different from its physical analogs. The pervasive use of cell phones in everyday life was also a factor in the Court's holding that cell phone data deserves greater privacy protection than other physical items. The Court observed that digital data is fundamentally different than traditional analog records, and is deserving of separate Fourth Amendment analysis:

> A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

Id. at 2489.

At the outset, the Court in *Riley* recognized that modern cell phones enable the creation and storage of an enormous amount of sensitive data. "The term 'cell phone' is itself misleading shorthand, many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone." *Riley*, 134 S. Ct. at 2489. The Court found that, in particular, the capacity of cell phones to store large aggregations of data implicated broader privacy interests than with physical containers. "[A] cell phone's capacity allows even just one type of information to convey far more than previously possible." *Id*. "A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." *Id*. Therefore, the Court's holding

was based on its conclusion that the aggregation of data can, and does, affect the Fourth Amendment privacy interest at stake.

The Court also noted that "there is an element of pervasiveness that characterizes cell phones," impacting the privacy interests at stake. *Id*. at 2490. "Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id*. And this pervasiveness changes the impact of the government's action on all citizens' privacy intersests. "Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." *Id*.

Although the Court did not consider in *Riley* whether the government's access to all telephone call records held by a service provider constitutes a "search," the Court's reasoning clearly undercuts the broad reading of *Smith v. Maryland* advocated by the Government, and provides lower courts with a basis to establish new privacy rules for digital records.

Consumers today routinely store their e-mails, photographs, notes, calendars, financial records, and other sensitive files on servers hosted and controlled by third party providers. Federal courts have held that these users have a reasonable expectation of privacy in their e-mails, even though third-party providers store the messages. *See United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). Major service providers already require that police obtain a warrant before

seeking stored e-mails, making the *Warshak* rule applicable for those services nationwide, and the DOJ has not challenged this shift in Fourth Amendment doctrine.

Under the Court's reasoning in *Riley*, the call detail records at issue in this case, collected in bulk by the National Security Agency, are also clearly deserving of privacy protection. The records are detailed and comprehensive, covering all calls processed by the provider over the last five years. The mobile and landline phones used to make these calls are also ubiquitous, as the Court recognized in *Riley*, and thus the collected call data contains information about nearly every American's calls and connections.

In fact, the bulk telephone records collected by the NSA reveal a great deal more information about social connections between citizens than any traditional pen register data could. But as the Court recognized in *Riley*, this aggregation of millions of records heightens the privacy harm to each user. *Riley*, 134 S. Ct. at 2489. And due to the ubiquity of cell phones in the United States, the volume of call data is much higher now than in 1979 before the emergence of mobile phones.[21] Location data, in particular, reveals sensitive information including a "comprehensive record of a person's public movements that reflects a wealth of

[21] As of January 2014, at least 90% of American adults have a cell phone, and 58% have a smartphone. PewResearch Internet Project, *Mobile Technology Fact Sheet* (2014), *available at* http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

detail about her familial, political, professional, religious, and sexual associations." *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

The lower court's broad reading of *Smith v. Maryland* is inconsistent with the Court's recent holding in *Riley*. Modern networks generate a wealth of detailed data about our communications, and the ability to analyze and extract sensitive personal information from that data implicates users' privacy interests in a way inconceivable in the 1970s. To argue that the disclosure of all telephone records of all telephone customers in the United States today is equivalent to the disclosure of the telephone records from a single telephone line in the 1970s is like equating the Hubble space telescope and the bottom of a glass jar because they both enlarge images. The collection and aggregation of private communications data by the NSA on a nationwide scale violates the reasonable expectations of privacy of everyday Americans.

CONCLUSION

Amicus respectfully requests this Court vacate the lower court's order dismissing the claims in this case and denying Appellant's motion for a preliminary injunction.

Respectfully submitted,

/s/ Marc Rotenberg

Marc Rotenberg
Counsel of Record
Alan Butler
Julia Horwitz
Jeramie Scott
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,717 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also 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 this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac 2011 in 14 point Times New Roman style.

Dated: September 9, 2014

/s/ Marc Rotenberg
Marc Rotenberg