13-50572

IN THE

United States Court of Appeals

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

—v.—

BASAALY MOALIN,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA
CASE NO. 10-CR-4246
HONORABLE JEFFREY T. MILLER, SENIOR DISTRICT JUDGE

BRIEF OF *AMICI CURIAE* BRENNAN CENTER FOR JUSTICE, AMERICAN LIBRARY ASSOCIATION, ELECTRONIC PRIVACY INFORMATION CENTER, FREEDOM TO READ FOUNDATION, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NINTH CIRCUIT FEDERAL AND COMMUNITY DEFENDERS, REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

MICHAEL PRICE*
BRENNAN CENTER FOR JUSTICE
AT NEW YORK UNIVERSITY
SCHOOL OF LAW
161 Avenue of the Americas
New York, New York 10013
(646) 292-8335

FAIZA PATEL
BRENNAN CENTER FOR JUSTICE
AT NEW YORK UNIVERSITY
SCHOOL OF LAW
161 Avenue of the Americas
New York, New York 10013
(646) 292-8325

**Counsel of Record*

Attorneys for Amici Curiae Brennan Center for Justice, American Library Association, and Freedom to Read Foundation

(*Counsel continued on inside cover*)

ALAN BUTLER
ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1718 Connecticut Avenue NW
Washington, DC 20009
(202) 483-1140

DAVID M. PORTER
CO-CHAIR, NACDL AMICUS COMMITTEE
801 I Street, 3rd Floor
Sacramento, California 95814
(916) 498-5700

BRUCE D. BROWN
KATIE TOWNSEND
HANNAH BLOCH-WEHBA
THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS
1156 15th Street NW, Suite 1250
Washington, D.C. 20005
(202) 795-9300

MICHAEL FILIPOVIC
FEDERAL PUBLIC DEFENDER
WESTERN DISTRICT OF WASHINGTON
1601 Fifth Avenue, Room 700
Seattle, Washington 98101
(206) 553-1100

TONY GALLAGHER
EXECUTIVE DIRECTOR
FEDERAL DEFENDERS OF MONTANA
104 Second Street South, Suite 301
Great Falls, Montana 59401
(406) 727-5328

LISA HAY
FEDERAL PUBLIC DEFENDER
DISTRICT OF OREGON
One Main Place
101 Southwest Main Street, Room 1700
Portland, Oregon 97204
(503) 326-2123

HEATHER ERICA WILLIAMS
FEDERAL PUBLIC DEFENDER
EASTERN DISTRICT OF CALIFORNIA
801 I Street, 3rd Floor
Sacramento, California 95814
(916) 498-5700

STEVEN GARY KALAR
FEDERAL PUBLIC DEFENDER
NORTHERN DISTRICT OF CALIFORNIA
Internal Box 36106
San Francisco, California 94102
(415) 436-7700

HILARY POTASCHNER
FEDERAL PUBLIC DEFENDER
CENTRAL DISTRICT OF CALIFORNIA
321 East Second Street
Los Angeles, California 90012
(213) 894-2854

REUBEN CAHN
EXECUTIVE DIRECTOR
FEDERAL DEFENDERS OF SAN DIEGO, INC.
The NBC Building
225 Broadway, Room 900
San Diego, California 92101
(619) 234-8467

JON M. SANDS
FEDERAL PUBLIC DEFENDER
DISTRICT OF ARIZONA
850 West Adams Street, Room 201
Phoenix, Arizona 85007
(602) 382-2800

RICH CURTNER
FEDERAL PUBLIC DEFENDER
DISTRICT OF ALASKA
601 West Fifth Avenue, Suite 800
Anchorage, Alaska 99501
(907) 646-3400

JOHN T. GORMAN
FEDERAL PUBLIC DEFENDER
DISTRICT OF GUAM
First Hawaiian Bank Building
400 Route 8, Room 501
Mong Mong, Guam 96901
(671) 472-4711

PETER WOLFF
FEDERAL PUBLIC DEFENDER
DISTRICT OF HAWAII
Prince Kuhio Federal Building
300 Ala Moana Boulevard,
Suite 7-104
Honolulu, Hawaii 96850

SAMUEL RICHARD RUBIN
DISTRICT OF IDAHO COMMUNITY
DEFENDER
702 West Idaho Street, Room 1000
Boise, Idaho 83702
(208) 331-5500

R.L. VALLADARES
FEDERAL PUBLIC DEFENDER
DISTRICT OF NEVADA
411 East Bonneville Avenue,
Room S 245
Las Vegas, Nevada 89101
(702) 388-6577

CORPORATE DISCLOSURE STATEMENT

Pursuant to 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.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Federal Statutes

Constitutional Provisions

Other Authorities

STATEMENT OF AMICI CURIAE[1]

The Brennan Center for Justice at New York University School of Law is a nonpartisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and constitutional limits on the government's exercise of power. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic surveillance and counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on privacy and First Amendment freedoms. As part of this effort, the Center has filed numerous *amicus* briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues. *See, e.g., Davis v. United States*, No. 15-146 (2015); *Matter of a Warrant (Microsoft Corp. v. United States)*, No. 14-2985-cv (2d Cir. 2015); *United States v. Carpenter*, Nos. 14-1572 & 14-1805 (6th Cir. 2015); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *United*

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for undersigned counsel, has authored this brief in whole or in part or contributed money toward the preparation of this brief. All parties have consented to the filing of this brief. This brief does not purport to represent the position of NYU School of Law.

States v. Cotterman, 709 F.3d 952 (9th Cir. 2013); *Hepting v. AT&T Corp*., 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig*., 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

The American Library Association (ALA) is the oldest and largest library association in the world providing advocacy, information, and resources to librarians and library users. It actively defends the right of library users to read, seek information, and speak freely as guaranteed by the First Amendment and vigorously supports Fourth Amendment rights to privacy as indispensable prerequisites to freedom of inquiry and other First Amendment freedoms.

The Electronic Privacy Information Center (EPIC) is a non-profit research center located in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, freedom of expression, human rights, and democratic values. Through its public education, litigation, and coalition efforts, EPIC advocates for strong constitutional limitations on domestic and electronic surveillance. EPIC has a particular interest in the NSA Metadata Program, having brought the first challenge in the Supreme Court, *In re EPIC*, 134 S. Ct. 638 (2013), and having testified before Congress on the need to limit the scope of the agency's surveillance activities. EPIC has also recently submitted an *amicus* brief in *Smith v. Obama*, No. 14-35555 (9th Cir.), a case currently pending before this Court, arguing that the court should not extend the

third party doctrine to modern metadata because the factual premises underlying *Smith v. Maryland* no longer apply. EPIC routinely participates as *amicus curiae* before federal and state appellate courts in cases involving emerging privacy and electronic surveillance issues. *See*, *e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Ganias*, No. 12-240 (2d Cir.); *In re National Security Letter*, Nos. 13-15957 & 13-16731 (9th Cir.); *In re US Application for CSLI*, 724 F.3d 600 (5th Cir. 2013); *State v. Earls*, 70 A.3d 630 (N.J. 2013); *Commonwealth v. Connolly*, 913 N.E.2d 356 (Mass. 2009).

The Freedom to Read Foundation is an organization established by the American Library Association to promote and defend First Amendment rights, foster libraries as institutions that fulfill the promise of the First Amendment, support the right of libraries to include in their collections and make available to the public any work they may legally acquire, and establish legal precedent for the freedom to read of all citizens, including the protection of readers' privacy rights as a means of securing the First Amendment right to receive information and engage in expressive activities.

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association working on behalf of criminal defense attorneys to promote justice and due process for those accused of crime or

misconduct. NACDL was founded in 1958. It has a nationwide membership of approximately 9,200 and up to 40,000 including affiliates' membership. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. The American Bar Association recognizes NACDL as an affiliated organization and awards it representation in the ABA House of Delegates.

NACDL is dedicated to advancing the proper, efficient, and just administration of justice and files numerous amicus briefs each year in this Court and other federal and state courts, addressing issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

The Ninth Circuit Federal and Community Defenders (the "Defenders") provide representation to the indigent accused in federal court in the Ninth Circuit pursuant to the Criminal Justice Act, 18 U.S.C. § 3006A. Offices administered by the Federal Public and Community Defenders employ over 250 lawyers whose exclusive practice is the representation of financially-eligible people both at trial and on appeal in this Circuit.

The Reporters Committee for Freedom of the Press is a voluntary, unincorporated association of reporters and editors that works to defend the First

Amendment rights and freedom of information interests of the news media. The Reporters Committee has provided assistance and research in First Amendment and Freedom of Information Act litigation since 1970.

INTRODUCTION

In 1967, exercising the right to privacy meant remembering to close the phone booth door, thus taking an affirmative act to exclude the "uninvited ear" from eavesdropping on the content of a conversation. *Katz v. United States*, 389 U.S. 347, 352 (1967). Some doors, however, cannot be closed. It is impossible to place a phone call without indicating to the phone company which lines to connect – a necessity that the Supreme Court mistook for a choice in *Smith v. Maryland*, 442 U.S. 735, 742 (1979). The result has been that a warrant is required for law enforcement to listen in on the content of the conversation, but not to obtain records about it from the phone company, often called phone "metadata." In recent years, however, this distinction between metadata and content has become increasingly untenable, and the so-called "third-party doctrine" associated with it has proven "ill suited to the digital age." *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). This brief explains why.

The phone record surveillance program at issue in this case is just the tip of the iceberg. Modern electronic communications generate massive amounts of metadata, leagues beyond the digits dialed in *Smith*. 442 U.S. at 741. As metadata has proliferated, so too has the government's appetite for obtaining it in bulk. The dragnet collection of Americans' phone call metadata by the National Security Agency ("NSA") was recently repudiated by Congress. *See* Uniting and

Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (USA FREEDOM Act). But the NSA also ran programs to collect Americans' e-mail and Internet metadata in bulk and a two-year pilot program to collect domestic cell phone location information. Indeed, at least one of these other programs appears to have a role in this case. (CR 345 at 23, Def. Mtn. New Trial) (describing a missed international phone call intercepted by unknown, independent means).[2] The Supreme Court, however, has never considered government surveillance of this nature or scope. *Smith* simply did not anticipate e-mail, cell phones, and mobile apps; nor did the Court consider the implications of making this data available to law enforcement – let alone in bulk – because neither the data nor the tools for analyzing it existed.

Today, communications metadata easily reveals lawful, First Amendment-protected activities in a way that was unimaginable when the Court decided *Smith* in 1979. It is a digital trail of past and present political associations, personal sympathies, and private affairs. It can reveal confidential relationships between reporters and sources, whistleblowers and watchdogs, as well as attorneys and clients. It implicates the kind of expressive and associational activities that the Framers sought to protect by including "papers" in the text of the Fourth

[2] "CR" refers to the Clerk's Record.

Amendment. This First Amendment nexus weighs heavily in favor of finding a reasonable expectation of privacy in communications metadata. Phone records, like all communications metadata, should be considered Fourth Amendment "papers," and by default, require a warrant for search or seizure.

Under the third-party doctrine, however, there is said to be no Fourth Amendment interest in such metadata because it is "voluntarily" conveyed to "third parties." *Smith*, 442 U.S. at 743–44; *United States v. Miller*, 425 U.S. 435, 442 (1976). Yet this doctrine appears increasingly anachronistic in the digital age, as the Supreme Court recently suggested. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). First, the "assumption of risk" rationale underlying the rule makes increasingly little sense, as exposing reams of metadata to third parties is an unavoidable feature of modern life. Second, the line between content and metadata has become increasingly beset by technical difficulties. Finally, the third-party doctrine is at odds with the way people share information, mistaking it for either completely secret or presumptively public and failing to account for individual decisions about privacy.

ARGUMENT

I. The Government Is Systematically Collecting Records of Phone Calls, Text Messages, E-Mails, and Other Digital Communications

The communications records at issue in this case are, at least in part, due to the NSA's program to collect domestic phone metadata under Section 215 of the

USA PATRIOT Act (the "215 Program"). 50 U.S.C. § 1861 (as amended by the USA PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 272 (2001)). Federal courts,[3] congressional leaders,[4] and a bipartisan oversight board appointed by the President[5] have all recognized the constitutional infirmity of the 215 Program, and Congress reformed the law in May 2015. *See* USA FREEDOM Act, 129 Stat. 268. The 215 Program is the best-known example of a post-9/11 shift to the wholesale collection of communications metadata, but it is hardly an isolated endeavor. As modern communications generate increasing amounts of metadata, the

[3] *See ACLU v. Clapper*, 785 F.3d 787, 818 (2d Cir. 2015) (holding that the 215 Program violated the Foreign Intelligence Surveillance Act); *Klayman v. Obama*, 957 F. Supp. 2d 1, 41-42 (D.D.C. 2013) (finding that that 215 Program is an unreasonable search under the Fourth Amendment), *vacated and remanded on other grounds*, 2015 WL 5058403, at *2 (D.C. Cir Aug. 28, 2015).

[4] *See, e.g.,* Press Release, Office of Sen. Patrick Leahy, Statement of Senator Patrick Leahy (D. Vt.), Ranking Member, Senate Judiciary Committee, On the Introduction of the USA Freedom Act of 2015 (Apr. 28, 2015), https://www.leahy.senate.gov/press/statement-of-senator-patrick-leahy-d-vt-ranking-member-senate-judiciary-committee-on-the-introduction-of-the-usa-freedom-act-of-2015 ("Relying on a deeply flawed interpretation of Section 215 ... the NSA has been indiscriminately sweeping up Americans' private telephone records for years. It is long past time to end this bulk collection program."); Letter from Rep. James Sensenbrenner to Eric J. Holder, Jr., U.S. Att'y Gen. (Sept. 6, 2013), http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf ("In passing Section 215, Congress intended to allow the government access to *specific* records. The administration's interpretation to allow for bulk collection is at odds with Congressional intent… The implications of this flawed interpretation are staggering.").

[5] Privacy and Civil Liberties Oversight Bd., *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 114-16 (2014) [hereinafter *PCLOB 215 Report*].

government's efforts to collect it in bulk are also expanding. Other NSA programs may also be at issue in this case, including the bulk collection of electronic communications under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") (CR 345 at 7), or under Executive Order ("EO") 12333. *See* Nat'l Sec. Agency, *Legal Fact Sheet: Executive Order 12333* (Jun. 19, 2013).[6] This Court's approach to the third-party doctrine should be mindful of the tremendous difference between the limited call records in *Smith* and the all-encompassing surveillance conducted by the NSA.

A. The 215 Program

The 215 Program remains operational until the USA FREEDOM Act takes effect on November 29, 2015. *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, No. BR 15-75, slip op. at 1 (FISA Ct. Jun. 29, 2015) ("Plus ça change, plus c'est la même chose, well, at least for 180 days."). It also differs substantially from the pen register at issue in *Smith* in both the quantity and nature of phone records collected and the quality of software available to analyze them. Most significantly, the program is "comprehensive" in scope. Decl. of Teresa H. Shea, Signals Intelligence Director, National Security Agency, ¶¶ 59-60, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013). It targets not just the

[6] *Available at* https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf.

records of a few calls over a few days, but billions of calls over the course of years. *PCLOB 215 Report* at 73. Moreover, the NSA uses powerful computer algorithms capable of interpreting this information in ways that would have been unfathomable decades ago. *Id.* at 26. Rapid changes in technology have enabled this tectonic shift while the law is playing catch-up.

Using the 215 Program, the NSA collects metadata for all calls to or from the United States carried by the nation's largest telecommunication carriers. *Id.* at 22. It obtains "call detail records" associated with millions of Americans on a daily basis, including 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.

Primary Order at 3 n.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, at *10 n.1 (FISA Ct. Aug. 29, 2013). IMSI and IMEI numbers are unique numbers associated with a particular telephone user or communications device. *PCLOB 215 Report* at 26 n.52. A "trunk identifier" provides information about where a phone connected to the network, revealing data that can locate the parties

within approximately a square kilometer. *See* Patrick Di Justo, *What the N.S.A. Wants to Know About Your Phone Calls*, New Yorker, Jun. 7, 2013.[7]

The NSA maintains a copy of this "telephony metadata" and keeps it for at least five years. *PCLOB 215 Report* at 25. And as detailed in Part II, the agency employs sophisticated software to analyze it with ease, revealing otherwise hidden personal connections. *Id.* at 26. Unlike the records in *Smith*, the 215 Program shows not only who called whom, but also the precise duration and time of each call (including missed calls), as well as the frequency and pattern of contact. *Id.* at 115-16 (describing the 215 Program as "dramatically broader than the practice approved by the Supreme Court in *Smith*, which was directed at a single criminal suspect and gathered 'only the numbers he dialed on his phone' during a limited period.").

For two years starting in 2010, the NSA also used its Section 215 authority for a program designed to collect domestic cell phone location information. Charlie Savage, *In Test Project, N.S.A. Tracked Cellphone Locations*, N.Y. Times, Oct. 2, 2013;[8] Ellen Nakashima, *NSA Had Test Project to Collect Data on Americans'*

[7] *Available at* http://www.newyorker.com/tech/elements/what-the-n-s-a-wants-to-know-about-your-phone-calls.
[8] *Available at* http://www.nytimes.com/2013/10/03/us/nsa-experiment-traced-us-cellphone-locations.html.

Cellphone Locations, Director Says, Wash. Post, Oct. 2, 2013.[9] Mobile devices generate constant streams of location data by wirelessly pinging nearby cellular towers and sending GPS signals. This data reveals a rich trail of individual movements over time, creating a map of activities and habits, regardless of whether the phone is ever used to make a phone call.[10] Although the program is no longer operational, there remains great uncertainty about whether the NSA is effectively replicating it under a different authority, such as one of those described below.

B. Other NSA Metadata Collection Programs

The 215 Program is far from unique, and it is likely not the only NSA program implicated in this case. (CR 345 at 23) Communications metadata consists of much more than telephone call records, and it is widely known that the NSA has created additional surveillance programs to capture and analyze it. The NSA is equipped to collect 94 different metadata "entity types" (including but not limited to call records) for a total of 20 billion "record events" each day. James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y.

---

[9] *Available at* https://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.

[10] *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary*, 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) [hereinafter Blaze Statement].

Times, Sept. 28, 2013.[11] Nearly all of this metadata is the product of interactions involving third parties, such as phone companies and Internet service providers. The enormous scope of these programs underscores the difference between the surveillance in *Smith* and the facts here, as well as the potential consequences of this Court's decision on the Section 215 Program.

According to a report by the NSA Inspector General, the NSA began its dragnet collection of Internet metadata in 2001 as part of the "President's Surveillance Program," unauthorized by warrant or court order. Office of the Inspector General, Nat'l Sec. Agency, *ST-09-0002 Working Draft* 34 (Mar. 24, 2009).[12] In 2004, the NSA decided to "transition" the program to court supervision using the pen register/trap and trace provisions ("PR/TT") of FISA. 50 U.S.C. §§1841-46; Charlie Savage & James Risen, *New Leak Suggests Ashcroft Confrontation Was Over N.S.A. Program*, N.Y. Times, Jun. 27, 2013.[13] Although many details remain classified, the NSA obtained authorization to collect Internet metadata in bulk, including the "to," "from," "cc," and "bcc" lines of e-mails, as well as the Internet-protocol ("IP") addresses used to transmit data. *See* [Redacted],

[11] *Available at* http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html.
[12] *Available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.
[13] *Available at* http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html.

No. PR/TT [Redacted], slip op. at 23 (FISA Ct. n.d.);[14] Dep't of Def., *Supplemental Procedures Governing Metadata Collection & Analysis* 1 (2004).[15] IP addresses can be used to track an individual's identity and location as well as monitor their Internet activity. *See Register.com v. Verio*, 356 F.3d 393, 409-10 (2d Cir. 2004). Although the NSA claims to have ended this program in 2011, the *Guardian* reports that Internet metadata is collected under other authorities – and that the NSA had processed more than a trillion records by the end of 2012. Glenn Greenwald & Spencer Ackerman, *How the NSA Is Still Harvesting Your Online Data*, Guardian, Jun. 27, 2013.[16]

Under Section 702 of FISA, for instance, the NSA collects the content of communications, including telephone calls and e-mails, as well as the associated metadata. *See* 50 U.S.C. § 1881a; Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 112 (2014).[17] Unlike the Section 215 Program, surveillance under Section 702 is intended to capture the communications of foreigners overseas, *see* 50 U.S.C. §§ 1881a(d)(1)(A),

---

[14] *Available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.
[15] *Available at* https://www.eff.org/files/2015/03/19/37-dod-supp-procedures-governing-comm-metadata.pdf.
[16] *Available at* http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.
[17] *Available at* https://www.pclob.gov/library/702-Report.pdf.

1881a(e)(1), 1801(h)(1), although it "incidentally" or "inadvertently" sweeps up a massive number of Americans' phone calls and e-mails. *See* Elizabeth Goitein and Faiza Patel, *What Went Wrong with the FISA Court*, Brennan Ctr. for Justice 3 (2015). [18] This is an inevitable feature given the volume of international communication between Americans and foreigners. *Id*. at 20 (noting that in 1980, the average American spent less than 13 minutes a year on international calls, compared with 4.5 hours in 2011 – not including communications via Skype, FaceTime, or other Internet-based providers). There are at least two large-scale Section 702 programs, one that taps into the hardware backbone of the Internet, *see* Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, Wash. Post, Jul. 10, 2013,[19] and another that collects communications content and metadata from major U.S. service providers, including Microsoft, Yahoo, Google, Facebook, AOL, Skype, YouTube, and Apple. *See NSA Slides Explain the PRISM Data-Collection Process*, Wash. Post, June 6, 2013.[20]

Finally, the NSA's largest surveillance programs are conducted under the authority of Executive Order ("EO") 12333. Nat'l Sec. Agency, *Legal Fact Sheet*,

---

[18] *Available at* https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

[19] *Available at* http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

[20] *Available at* http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (updated Jul. 10, 2013).

supra, at 1. The EO underpins NSA bulk surveillance programs that monitor overseas communications, both content and metadata. These programs are not court-authorized and there has been little in the way of Congressional oversight. But the broad swath of NSA activities under EO 12333 means that the communications of many Americans are inevitably acquired as they travel abroad or communicate with foreigners. Even purely domestic communications can be swept up if they are transmitted to or stored on a server overseas. The NSA shares this information with nearly two dozen other government agencies through a "Google-like" search engine, built to share more than "850 billion records about phone calls, emails, cellphone locations, and internet chats." Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, Intercept, Aug. 25, 2014.[21]

II. Communications Metadata Is Fourth Amendment "Papers"

Communications metadata is a digital log of expressive and associational activities. While the government asserts that it does not include the "content" of a conversation, metadata is still incredibly revealing. Even in limited quantities, it can signal the significance of a communication. One call to a reporter can reveal a confidential source, corroding the ability to report news of public interest. One call to a defense lawyer can undermine the confidentiality of attorney-client

[21] *Available at* https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

communications. In aggregate, metadata is even more potent and easily manipulated to extrapolate social and political networks, personal beliefs, and private associations. The history and purpose of the Fourth Amendment dictate a duty to safeguard such First Amendment affairs from unreasonable government interference. Communications metadata is the modern equivalent of Fourth Amendment "papers," and it follows that a warrant generally should be required to search or seize it.

A. Communications Metadata Is Revealing, Even in Limited Quantities

Metadata is personal data, and even in limited quantities, it can be a telltale sign of social, political, and religious activities. Phone call records, for example, can be a proxy for call content if dialing a hotline for victims of rape or domestic abuse, suicide prevention, or addiction and substance abuse. *See* Decl. of Edward W. Felten, *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Aug. 23, 2013), ECF No. 27 ("Felten Decl."), 14-15. Calls to such single-purpose lines are common; they are the "1-800" numbers occupying billboards and newspaper ads. Information about a single call to a reporter, tip-line, or agency inspector general could identify a whistleblower and inhibit freedom of the press. *Id.* at 15. While the NSA's Section 215 program collects only numbers and not the names of individuals or entities associated with them, making this connection is trivially easy. *Id*. at 7.

The same is true for text message metadata. One text to a dedicated number is all it takes to subscribe to mobile alerts from an advocacy organization or protest group. *See, e.g.,* Amy Gahran, *Mobile Tools for Protests – Then and Now*, CNN, Oct. 10, 2011 (describing the role of text message alert systems as the primary tool for protest coordination during the 2004 Republican National Convention protests in New York).[22] One message is all it takes to donate money to a charity, church, or political candidate. *See, e.g.,* Mario Trujillo, *Twitter Rolls Out Donate Button For Political Campaigns*, The Hill, Sept. 15, 2015;[23] Felten Decl. at 16 ("For example, by sending the word HAITI to 90999, a wireless subscriber can donate $10 to the American Red Cross."). One message is all it takes for a journalist to speak to a trusted source or for a client to contact a defense lawyer.

Metadata generated by online browsing can be as revealing as content, if not more so. Knowing the web address (or "URL") visited is often the functional equivalent of accessing content. *See, e.g.,* Ashley Madison, https://www.ashleymadison.com/ (last visited Oct. 22, 2015) ("Life is short. Have an affair."). But web browsing records also provide context – additional metadata about when, where, and how a website was viewed. *See* Matt Blaze, *Phew, NSA Is*

[22] *Available at* http://www.cnn.com/2011/10/10/tech/mobile/mobile-tools-for-protest/.
[23] *Available at* http://thehill.com/policy/technology/253649-twitter-rolls-out-donate-button-for-political-campaigns.

Just Collecting Metadata. (You Should Still Worry), Wired, Jun. 19, 2013.[24] Even in isolation, the metadata can indicate intent: Was the webpage viewed during the day from a computer at a government research facility, or was it viewed from a personal computer at an odd hour of the night?

Mobile phones also generate location metadata on a frequent and automatic basis, regardless of whether the device is actively in use. Blaze Statement, *supra*, at 6. As in the GPS-tracking context, even short-term monitoring of this location information can reveal activities of "indisputably private nature" like a call or visit to the "psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 909 N.E.2d 1195, 1999 (N.Y. 2009)).

B. Metadata Is Especially Revealing in Aggregate

Communications metadata is invasive in isolation, but in aggregate, it is even more revealing of First Amendment activity. It is highly structured, which makes it easy to collect, store, and analyze with computer software. Phone numbers are standardized and expressed in a predictable format, as are e-mail addresses, IP addresses, and URLs – no human interpretation required. *See* Felten

[24] *Available at* http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/.

Decl. at 7-8. As a result, it is relatively simple to "[superimpose] our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups" and quickly "[paint] a picture that can be startlingly detailed." *Id.* at 2. These staccato signals can even identify the strength of relationships and the structure of organizations. Just a cursory analysis can distinguish the organizers of a grassroots movement from casual participants. More detailed study can show "if opposition leaders are meeting, who is involved, where they gather, and for how long." Jane Mayer, *What's the Matter With Metadata?*, New Yorker, June 6, 2013, (quoting interview with Prof. Susan Landau, former privacy analyst at Google).[25]

This is not idle speculation. The NSA uses communications metadata to conduct "contact chaining," a process showing the phone numbers or e-mail addresses that a "seed" number or e-mail address has contacted or attempted to contact as well as those who are in touch with the seed's contacts. *PCLOB 215 Report* at 8-9. A single, "three-hop" analysis of this type would yield 2.5 million phone numbers, assuming each person contacts 40 unique people. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The NSA Three-Hop* n.3, Dec. 9, 2013.[26] It is a matter of mouse clicks to build a "social graph" identifying a substantial portion of

[25] *Available at* http://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata.
[26] *Available at* http://webpolicy.org/2013/12/09/metaphone-the-nsa-three-hop/.

a group's membership, donors, sources, and political supporters. Felten Decl. at 17-20. Because of the potential for such aggregation and analysis, digital metadata is fundamentally different from the pen register at issue in *Smith*. *See* Alan Butler, *Get A Warrant: The Supreme Court's New Course for Digital Privacy Rights after* Riley v. California, 10 Duke J. of Const. L. & Pub. Policy 83, 103 (2014) (describing the *Smith* Court's understanding of a pen register, which at the time recorded numbers on a paper tape and was incapable of determining whether any call was even completed).

C. Communications Metadata Is The Modern Equivalent of Fourth Amendment "Papers"

Communications metadata implicates the same kind of expressive and associational activities that the Fourth Amendment was designed to protect. By giving "papers" equal billing with "persons," "houses," and "effects," the Founding Fathers indicated that courts have a special obligation to safeguard First Amendment information from unreasonable searches and seizures. *See* U.S. Const. amend. IV; *Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kan. City, Mo.*, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); *Stanford v. Texas*, 379 U.S. 476, 482 (1965) (describing the history of the Fourth Amendment as "largely a history of conflict between the Crown and the press"). Consequently, the Supreme

Court has consistently recognized a strong Fourth Amendment interest where First Amendment concerns are at stake, holding that there is a reasonable expectation of privacy in this information, almost by definition. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); *Walter v. United States*, 447 U.S. 649, 655 (1980) ("When the contents of the package are books or other materials arguably protected by the First Amendment, and when the basis for the seizure is disapproval of the message contained therein, it is especially important that [the warrant] requirement be scrupulously observed."); *see also Maryland v. Macon*, 472 U.S. 463, 468 (1985) ("The First Amendment imposes special constraints on searches for and seizures of presumptively protected material."). This Court, therefore, should regard communications metadata as if it were considering the privacy of papers in a desk drawer. In the digital age, there is no meaningful distinction.

The Fourth Amendment was designed to safeguard individual liberty and free expression, as the Supreme Court has long recognized. *See Marcus*, 367 U.S. at 724-729; *Stanford*, 379 U.S. at 482; *Lopez v. United States*, 373 U.S. 427, 469–70 (1963) (Brennan, J., dissenting) ("[W]e must bear in mind that historically the search and seizure power was used to suppress freedom of speech and of the

press . . . ." (internal citations omitted)). It was intended to serve as a barrier to government overreach and as a catalyst for freedom of speech and freedom of association, essential ingredients for a robust democracy. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Nat'l Security L. & Pol'y __, *13 (forthcoming 2015).[27] Accordingly, the Court has required that the Fourth Amendment be applied with "scrupulous exactitude" when significant First Amendment rights are at stake. *Stanford*, 379 U.S. at 485; *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). This means that a search or seizure of "materials presumptively protected by the First Amendment" must be made pursuant to a warrant supported by probable cause. *See New York v. P. J. Video*, 475 U.S. 868, 873-75 (1986) ("We have long recognized that the seizure of films or books on the basis of their content implicates First Amendment concerns not raised by other kinds of seizures"); *Roaden v. Kentucky*, 413 U.S. 496, 504 (1973) (requiring a warrant to seize an allegedly obscene film because "[t]he setting of a bookstore or the commercial theater ... invokes such Fourth Amendment warrant requirements"); *Stanford Daily*, 436 U.S. at 565 (recognizing that courts must "apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."). Indeed, the Supreme Court reinforced this understanding recently in *Riley v. California*,

[27] *Available at* http://jnslp.com/wp-content/uploads/2015/06/Rethinking-Privacy.pdf.

requiring a warrant for the search of a cell phone incident to arrest because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated" by most physical searches, exposing to the government "far *more* than the most exhaustive search of a house." 134 S. Ct. 2437, 2488-91 (2014).

Communications metadata has such significant First Amendment expressive and associational implications that it demands Fourth Amendment protection, no less than pamphlets or hard copy letters. That protection is realized in the warrant requirement, which serves as a check on unreasonable government searches and seizures. Consequently, the presumption should be that a warrant is needed to search or seize private metadata unless it has been publicly disclosed. In the digital age, there is no good reason for treating metadata differently from other kinds of Fourth Amendment "papers."

III. Why the Third-Party Doctrine Is "Ill-Suited to the Digital Age"

The government argues that there is no privacy interest in communications metadata because it is disclosed to third-party service providers – here, the phone company. (CR 355 at 11-12, Resp. Opp. Mtn. New Trial) But the third-party doctrine of 1979 is "ill suited to the digital age." *Jones*, 132 S. Ct. at 957 (Sotomayor, J. concurring). The doctrine rests on outdated expectations about the "assumption of risk"; it relies on the vanishing distinction between metadata and

content; and it fails to account for the reality of how people share information today.

A. The "Assumption of Risk" Equation Has Changed

The third-party doctrine rests on the rationale that people "assume the risk" their data will be divulged to police if it is "voluntarily conveyed" through a third-party service provider. *Smith*, 442 U.S. at 745. This presumption, however, rests on an untenable concept of "voluntariness." In the digital age, there is no practical alternative to third-party providers, no option to truly mask metadata. Closing the telephone booth door to exclude the "uninvited ear," *Katz*, 389 U.S. at 352, is a meaningless exercise if the metadata is open to the uninvited eye.

Unlike in 1979, we all leave a digital trail of past and present political associations, personal sympathies, and private affairs in the form of metadata held by third-party service providers. *See* Felten Decl. at 11-12 ("[I]t is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats."). Exposing this information to third parties is an unavoidable feature of modern life, not a reasoned decision to subject it to police scrutiny. Of course, even at the time of *Smith*, it was impossible to avoid conveying some information to the phone company. 442 U.S. at 742. But comparing phone records in 1979 to communications metadata in 2015 is like "saying a ride on horseback is materially

indistinguishable from a flight to the moon." *See Riley*, 134 S. Ct. at 2484; *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (distinguishing the search of a laptop from the search of hand luggage) ("The point is technology matters.").

Metadata today is so persistent, so prevalent, and so pervasive – and the technology available to derive meaning from that metadata so advanced – that the only way to avoid authoring a digital autobiography in the form of third-party records is to stop communicating electronically. But in 2015, it is unreasonable to require Americans to stop communicating by phone or online if they desire privacy. Indeed, as the Supreme Court has repeatedly recognized, the privacy of such communications is essential to the exercise of First Amendment freedoms. *See City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."); *Riley*, 134 S. Ct. at 2484 ("[M]odern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy"); *see also United States v. Cooper*, No. 13-cr-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015) (unpublished) (cell phones are "ubiquitous, and for many, an

indispensible [sic] gizmo to navigate the social, economic, cultural, and professional realms of modern society.").

The sheer volume and inescapability of these third-party records, combined with the development of sophisticated software to analyze them, changes the "assumption of risk" equation in a fundamental way. Not only is the creation of third-party records unavoidable, but it is also simple to infer otherwise private expressive and associational activities from them. In 1979, such First Amendment information would have been practically obscured from phone operators, but in 2015, it is trivial to uncover patterns using a computer program. *See* Felten Decl. at 7-11. Regardless of whether phone users in 1979 voluntarily "assumed the risk" of disclosing the numbers they dialed to the police, it is not reasonable to conclude that individuals today voluntarily "assume the risk" of disclosing their religion, political affiliation, or sexual preferences to the government by communicating digitally. There is no alternative in a free and open society.

B. The Distinction Between Content and Metadata Is Not Sound

Courts do not apply the third-party doctrine to communications content, *Katz*, 389 U.S. at 352, even though content, like metadata, is transmitted and stored by third parties. This disparate treatment owes to the illusion of a firm distinction between content and metadata that has proven increasingly unsustainable. The

government seeks to draw a bright line, but the reality today is far more murky and malleable.

The technological boundary between "metadata" and "content" is a matter of computer rules that can change without notice at any time. *See* Steven M. Bellovin, *Submission to the Privacy and Civil Liberties Oversight Board: Technical Issues Raised by the § 215 and § 702 Surveillance Programs* 5 (2013).[28] "Metadata" is simply the information about a communication that the communications facilitator records, sometimes by necessity but increasingly by choice. For example, Internet service providers do not need to know what a person is doing online in order to connect one computer to another. But they now routinely monitor and filter certain "ports" associated with specific kinds of activity (e-mail, web browsing, etc.) to control spam, prevent hacking, and enforce their terms of service. *Id.* at 6. This would be equivalent to the phone company keeping tabs on the office extensions people dial or the menu options they select after connecting to a main number, information that would require a warrant for law enforcement access. *See In re U.S. for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices*, 515 F. Supp. 2d 325, 336 (E.D.N.Y. 2007) (finding a reasonable expectation of privacy in "post-cut-through dialed digits").

[28] *Available at* https://www.cs.columbia.edu/~smb/papers/PCLOB-statement.pdf.

Some of the information collected encompasses what any reasonable observer would consider to be (or, at least, to reflect) content. A URL can be likened to delivery instructions for Internet service providers, specifying the website requested and the data to be transmitted. But as discussed in Part II, a single URL also points to specific text, pictures, or videos, the content of which is easily ascertained. Every Google search, for example, generates a unique URL containing the terms of the search itself (e.g., www.google.com/search?q=rethinking+privacy…). *See* Price, 8 J. Nat'l Security L. & Pol'y, at *44; *In re Application of U.S. for an Order Authorizing Use of a Pen Register & Trap On (xxx) Internet Serv. Account/User Name, (xxxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005). As a result, there may be no meaningful distinction between content and metadata, as this Court has repeatedly recognized. *See In re Zynga Privacy Litigation*, 750 F.3d 1098, 1108-09 (9th Cir. 2014) ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication."); *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2007) ("Surveillance techniques that enable the government to determine ... the [URL] of the pages visited might be more constitutionally problematic. A URL ... identifies the particular document within a website that a person views and thus reveals much

more information about the person's Internet activity."); *see also* U.S. Dep't of Justice, U.S. Attorney's Manual, Title 9-7.500 (requiring U.S. Attorneys to consult with an expert before obtaining URL information).

Even the NSA had great difficulty separating metadata from content, leading to serious compliance problems with its bulk collection of Internet metadata under the PR/TT program. *See* [Redacted], No. PR/TT [Redacted], slip op. at 21 (FISA Ct. n.d.) ("'[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection").[29] Indeed, the Foreign Intelligence Surveillance Court was not persuaded that metadata and content are mutually exclusive categories of information, identifying forms of information that defy such simple categorization, such as a URL. *Id.* at 31-32. The court observed, "In the context of person-to-computer communications like the interactions between a user and web-mail service provider, ... determining what constitutes contents can become 'hazy.'" *Id.* at 35 (citing 2 LaFave, *et al.* Criminal Procedure § 4.6(b) at 476 ("[W]hen a person sends a message to a machine, the meaning of 'contents' is unclear."). Whatever analytic value the distinction between content and metadata once held, it has quickly lost its force for Fourth Amendment purposes.

[29] *Available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf

C. The Third-Party Doctrine Is Incompatible with Modern Communications

The third-party doctrine is an exceedingly blunt instrument. It divides the world in half: data is either completely secret or it is not private. But in practice, the privacy of communications metadata is not an all-or-nothing endeavor. Some metadata may be intended for public consumption, as when adding geolocation information to a Tweet. *See* Twitter, *FAQs About Adding Location to Your Tweets*, https://support.twitter.com/articles/78525 (last visited Oct. 30, 2015). On the other hand, metadata may be intended for a limited audience, or for no one at all – the reason e-mail has a "bcc" option. Advocacy organizations, including *Amici*, e-mail their supporters en masse, but they also take care to avoid disclosing their distribution list, even to intended recipients. Political candidates send mass e-mails to organize and solicit votes, but they do not (usually) indicate who else received a copy. Individually, there are countless personal reasons for wanting to "bcc" someone or omit location information. The point is that people may choose to keep certain data private even as they make other data public, a reality that the third-party doctrine is not equipped to handle.

The third-party doctrine disregards privacy decisions by treating metadata as if it were public information. In the digital age, however, decisions about how widely to share this data are immensely important. The terrain of sharing that exists between the extremes of secret and public is "the stuff of friendship and

familial bonds, of business and professional relationships, and of political and religious associations." Price, 8 J. Nat'l Security L. & Pol'y at *34. The ability to control access to this information is essential to a free and democratic society. *See NAACP v. Alabama* ex rel. *Patterson*, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs."); *see also Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 91–93 (1982); *Shelton v. Tucker*, 364 U.S. 479, 488 (1960); *Bates v. Little Rock*, 361 U.S. 516, 523–24 (1960).

In this light, several courts have rejected the third-party doctrine in the context of cell-phone location metadata. *See, e.g., United States v. Graham*, 796 F.3d 332, 360 (4th Cir. 2015), *rehearing en banc granted*, ___Fed. Appx.___, 2015 WL 6531272 (4th Cir. 2015); *In re Application for Tel. Info. Needed for a Criminal Investigation*, ___F. Supp. 3d___, 2015 WL 4594558, at *23 (N.D. Cal. Jul. 29, 2015); *Cooper*, 2015 WL 881578, *8; *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected."); *see also Commonwealth v. Augustine*, 4 N.E.3d 846, 866 (Mass. 2014), 4 N.E.3d at 866;

State v. Earls, 70 A.3d 630, 644 (N.J. 2013). As the Fourth Circuit recently explained:

> *Smith* and *Miller* do not endorse blind application of the doctrine in cases where information in which there are clearly reasonable privacy expectations is generated and recorded by a third party through an accident of technology. The third-party doctrine is intended to delimit Fourth Amendment protections where privacy claims are not reasonable—not to diminish Fourth Amendment protections where new technology provides new means for acquiring private information.

Graham, 796 F.3d at 360. Indeed, these courts now find strong support for their position in the Supreme Court's emerging approach to privacy in the digital age, as exemplified by the recent decisions in *Jones* and *Riley*.

In *Jones*, the Court held that a Fourth Amendment search occurred when the police attached a GPS tracker to a suspect's car and monitored it for 28 days. 132 S. Ct. at 949. The opinion of the court centered on the physical trespass involved in affixing the GPS device, but five Justices also concluded that the monitoring itself violated the Fourth Amendment. *Id.* at 958, 964 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring); *id.* at 955 (Sotomayor, J. concurring). Justice Sotomayor pointed to the "wealth of detail" about "familial, political, professional, religious, and sexual associations" capable of being revealed by the location information. *Id*. Moreover, she recognized that this concern is not confined to GPS tracking, but applies to third-party records too, noting that "[p]eople disclose the phone numbers that they dial or text to their cellular providers; the URLs that they

visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers." *Id.* at 957.

In *Riley*, the Court held that a warrant is required to search a cell phone incident to arrest, citing the volume and sensitivity of the data it contains. 134 S. Ct. at 2489-90, 2493. The justices were alarmed that a warrantless search would yield not only text messages and emails, but also "[h]istoric location information" – a form of metadata – which "can reconstruct someone's movements down to the minute, not only around town by also within a particular building." *Id.* at 2490. The opinion also focused on the revealing nature of information that individuals enter into their "apps" – information that, by definition, is shared with a third party (*i.e.*, the app provider). *Id.* Citing Justice Sotomayor in *Jones*, the Court determined that such information is qualitatively different from a search of physical records alone, capable of revealing "an individual's private interests or concerns" and detailed information about protected First Amendment activities. *Id.*

The common denominator in these decisions is that the data reveals the kind of protected expressive and associational information the Framers sought to shield from warrantless government interference. The *Riley* Court was not just concerned with the "content" we store and access on our phones, but also the metadata we generate as a result of our daily activities and share with third parties. It was for

this reason that Justice Sotomayor suggested in *Jones* that "it may be necessary to reconsider" the third-party doctrine altogether as a rule "ill suited to the digital age." *Jones*, 132 S. Ct. at 957.

CONCLUSION

Systematic surveillance that subverts First Amendment values is exactly what the Framers abhorred. The third-party doctrine advanced in *Smith* may have been appropriate for phone calls in 1979, but it is a poor match for the digital age and the sweeping surveillance programs operated by the NSA. This Court should decline to extend it here.

Dated: November 5, 2015

Respectfully submitted,

/s/ Michael Price

Michael Price
BRENNAN CENTER FOR JUSTICE
AT NEW YORK UNIVERSITY
SCHOOL OF LAW
161 Avenue of the Americas
New York, New York 10013
(646) 292-8335

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,994 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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 this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: November 5, 2015

/s/ Michael Price
Michael Price

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on November 5, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accompanied by the appellate CM/ECF system.

Dated: November 5, 2015

/s/ Michael Price

Michael Price

Counsel for Amici Curiae