14-42

IN THE

United States Court of Appeals for the Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellants,

– against –

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF FOR THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK AS AMICUS CURIAE SUPPORTING PLAINTIFFS-APPELLANTS' BRIEF

Jonathan Hafetz
Chair, Task Force on National Security
and the Rule of Law
ASSOCIATION OF THE BAR OF
THE CITY OF NEW YORK
42 West 44th Street
New York, NY 10036
Tel.: (212) 382-6600

Gary D. Sesser
Stephen L. Kass
Michael Shapiro
Laura A. Zaccone
CARTER LEDYARD & MILBURN LLP
Two Wall Street
New York, NY 10005
Tel.: (212) 732-3200
Fax: (212) 732-3232

Counsel for the Association of the Bar of the City of New York

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes and Rules

Journals and Periodicals

Reports, Treatises, and Books

Other Authorities

The Association of the Bar of the City of New York ("Association") respectfully submits this amicus curiae brief in support of the appellants. All parties have consented to the filing of this brief.

INTEREST OF AMICUS CURIAE[1]

Founded in 1870, the Association is a professional organization of more than 24,000 members. The Association's stated mission includes "harnessing the expertise of the legal profession to identify and address legal and public policy issues in ways that promote law reform, ethics and the fair and effective administration of justice, and a respect for the rule of law at home and abroad."[2] Through its many standing and special committees and task forces, including the Task Force on National Security and the Rule of Law, the Association educates the Bar and the public about legal issues pertaining to the rule of law and the role of the Constitution in the face of real and continuing threats to our nation's security.

As one of the nation's oldest and largest bar associations, the Association has long had a significant interest in maintaining a strong and effective judicial branch with the ability to ensure the rule of law. The Association believes that individual liberties—including the right to seek judicial review of allegedly illegal government

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5) and Local Rule 29.1(b), counsel for amicus affirms that no counsel for a party authored this brief, in whole or in part, and that no person other than amicus and its counsel made a monetary contribution to its preparation or submission.

[2] *See About the New York City Bar Association*, N.Y. CITY BAR, http://www.nycbar.org/about-us/overview-about-us (last accessed Mar. 12, 2014).

action—need not be subverted during times of war or other crises. It believes that national security can be achieved without prejudice to the constitutional rights that are at the heart of our democracy.

Moreover, the Association's members have a professional responsibility to uphold the attorney-client privilege and to protect the confidential information of their clients.[3] This responsibility "fosters the open dialogue between lawyer and client that is deemed essential to effective representation." *Tekni-Plex, Inc. v. Meyner & Landis*, 674 N.E.2d 663, 667 (N.Y. 1996) (quoting *Spectrum Sys. Int'l Corp. v. Chem. Bank*, 581 N.E.2d 1055, 1059 (N.Y. 1991)). Therefore, recent news reports that a U.S. law firm's communications with its foreign government client were monitored by an ally of the National Security Agency (NSA) are of grave concern to the Association and to lawyers throughout the country.[4]

The Association submits that the NSA's bulk telephony metadata collection program—which has involved wholesale collection of certain information "for substantially every telephone call in the United States" since May 2006, *Am. Civil Liberties Union v. Clapper*, No. 13-cv-03994 (WHP), slip op. at 10, 12 (S.D.N.Y. Dec. 27, 2013)—must be accorded Fourth Amendment protection. While the court below recognized that this case involves the "natural tension between protecting the nation

[3] N.Y. RULES OF PROF'L CONDUCT R. 1.6.

[4] *See* James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES (Feb. 15, 2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=0.

and preserving civil liberty," *id.* at 2, it inappropriately applied the third-party doctrine and found that the plaintiffs had no legitimate expectation that sensitive information—relating to every telephone call they made or received over a period of years—would be private. For the reasons stated below—including qualitative changes in computerized communications and surveillance technology since the Supreme Court applied the third-party doctrine in 1979—the Association submits that the court below wrongly removed the Fourth Amendment from the analysis in balancing the "natural tension" between national security and civil liberties, *see id.*, and by doing so, compromised the fundamental right of privacy that is at the heart of both individual liberty and the rule of law.

PRELIMINARY STATEMENT

Since at least 2006,[5] the NSA has been collecting and analyzing telephone metadata for domestic calls made wholly within the United States. The government contends that Section 215 of the USA PATRIOT Act[6] authorizes the NSA to obtain FISA[7] court orders compelling telecommunications companies to produce "all call detail records or 'telephony metadata,'" or "comprehensive communications routing information"—including the originating and terminating number, the time and

[5] According to news reports, the NSA actually began collecting bulk phone and email metadata from millions of Americans in 2001, without court approval and with the cooperation of some of the largest American telecommunications companies. *See Why Justice Lawyers Defied President Bush*, NEWSWEEK (Dec. 12, 2008), http://www.newsweek.com/why-justice-lawyers-defied-president-bush-83515.

[6] Section 215 is codified at 50 U.S.C. § 1861.

[7] Foreign Intelligence Surveillance Act.

duration of each call, the international mobile subscriber identity (IMSI) and international mobile equipment identity (IMEI) of the devices (i.e., unique numbers that identify the user making or receiving the call), the trunk identifier (i.e., a number that provides a geographic data point on calls), and telephone calling-card numbers. The NSA's collection of call records is comprehensive—reaching substantially every phone call made through every major telecommunications service provider in the United States.

Upon a certification by the NSA that there is reasonable suspicion to believe that a phone number is associated with particular terrorist activity, the FISA court then allows NSA analysts to query the entire database of telephone numbers, using the "seed" telephone numbers or other telephone identifiers. The queries may include "contact chaining" or "hops"—looking at numbers one, two, or three steps removed from the suspicious identifier. Despite FISC orders limiting queries of the database to approved identifiers, the NSA has not always complied with those directives.[8]

While recognizing the "natural tension between protecting the nation and preserving civil liberty," the court below erred in applying the third-party doctrine and

[8] *See Klayman v. Obama*, 957 F. Supp. 2d 1, 18 (D.D.C. 2013) (noting that "[a]fter reviewing the Government's reports on its noncompliance, Judge Reggie Walton of the FISC concluded that the NSA had engaged in 'systematic noncompliance' with FISC-ordered minimization procedures over the preceding three years, since the inception of the Bulk Telephony Metadata Program, and had also repeatedly made misrepresentations and inaccurate statements about the program to the FISC judges") (citing Order, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9150913, at *2-5 (FISA Ct. Mar. 2, 2009)).

concluding that the ACLU had no reasonable expectation of privacy concerning information on every phone call it made or received over a period of years. The Association submits that the NSA's bulk telephony metadata collection program constitutes a "search" within the meaning of the Fourth Amendment to the Constitution and should be subject to Fourth Amendment scrutiny. Given the transformational changes in communications, information, and surveillance technology over the past three decades, the mere fact that the ACLU's phone calls are facilitated by a telecommunications provider does not eliminate its legitimate expectation of privacy or take the NSA's wholesale collection of telephone metadata outside of Fourth Amendment protection.

ARGUMENT

I. The NSA's Mass Collection of Phone Metadata Is a Search Under the Fourth Amendment.

The Fourth Amendment establishes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. In 1967, the Supreme Court interpreted this language as protecting "people, not places." *Katz v. United States*, 389 U.S. 347, 353 (1967). In Justice Harlan's formulation, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-52 (Harlan, J., concurring).

Thus, Fourth Amendment protections apply where (1) "a person [has] exhibited an actual (subjective) expectation of privacy" and (2) this expectation is "one that society is prepared to recognize as [objectively] 'reasonable.'" *Id.* at 360-61.

A. The ACLU Subjectively Expected That Its Phone Metadata Would Remain Private and That Expectation Was Objectively Reasonable.

The ACLU has a subjective expectation of privacy in its telephony metadata. *See* Complaint ¶¶ 24-27, *Am. Civil Liberties Union v. Clapper*, No. 13-cv-03994 (S.D.N.Y. June 11, 2013). ACLU staff frequently places calls to, and receive calls from, individuals in precarious situations. Often, the mere occurrence of these communications is sensitive or confidential. *See* Declaration of Steven R. Shapiro ¶¶ 4, 8, *Am. Civil Liberties Union v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Aug. 26, 2013) ("Shapiro Declaration"). Accordingly, the ACLU treats its telephony metadata as sensitive, and takes measures to protect its communications from surveillance by the government and third parties.[9] *See* Shapiro Declaration ¶ 5. While ACLU staff uses

[9] According to several polls, most Americans agree that their phone metadata should be secure from long-term recording and aggregation by the government. *See, e.g.*, PEW RESEARCH CTR., FEW SEE ADEQUATE LIMITS ON NSA SURVEILLANCE PROGRAM (July 26, 2013), http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf; Stephen Braun & Jennifer Agiesta, *Public Doubts Rise on Surveillance, Privacy: Poll*, HUFFINGTON POST (Sept. 10, 2013), http://www.huffingtonpost.com/2013/09/10/surveillance-poll_n_3903229.html ("Some 56 percent oppose the NSA's collection of telephone records for future investigations even though they do not include actual conversations."); Frank Newport, *Americans Disapprove of Government Surveillance Programs*, GALLUP POLITICS (June 12, 2013), http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx. *See also* Press Release, Office of Sen. Ron Wyden, Wyden Statement on Alleged Large-Scale Collection of Phone Records (June 6, 2013), http://www.wyden.senate.gov/news/press-releases/wyden-statement-on-alleged-large-scale-collection-of-phone-records ("Collecting this data about every single phone call that every American makes every day [is] a massive invasion of Americans' privacy.").

encryption software to protect the substance of its communications, the ACLU is aware of no security technology that would shield its telephony metadata from the type of mass surveillance at issue here. *See* Declaration of Professor Edward W. Felten ¶¶ 30, 33-37, *Am. Civil Liberties Union v. Clapper*, No. 13-cv-03994 (S.D.N.Y. Aug. 26, 2013) ("Felten Declaration").

Indeed, "it 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." Felten Declaration ¶ 30. As the Felten Declaration makes clear,

> Mobile phones are today ubiquitous, and their use necessarily requires reliance on a service provider to transmit telephone calls, text messages, and other data to and fro. These communications inevitably produce telephony metadata, which is created whenever a person places a call. *There is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether.*

Felten Declaration ¶ 37 (emphasis added).

The ACLU's expectation that its telephony metadata would be free from the government's long-term collection and aggregation is objectively reasonable. In determining whether a privacy expectation is reasonable, courts have considered societal expectations, particularly when confronted with new technologies. *See City of Ontario, Cal. v. Quon*, 560 U.S. 746, 759-60 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . [T]he Court would have difficulty predicting how employees' privacy expectations will be shaped by those

changes or the degree to which society will be prepared to recognize those expectations as reasonable."); *Georgia v. Randolph*, 547 U.S. 103, 111 (2006) (finding search based on spouse's consent, given over the target's objection, unreasonable based on "widely shared social expectations" and "commonly held understanding[s]"); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (recognizing that technological advances must not be permitted to erode society's expectation in the "degree of privacy against government that existed when the Fourth Amendment was adopted").

Phone communications, particularly over a mobile phone,[10] are so pervasive today "that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *Quon*, 560 U.S. at 760. *See Commonwealth v. Augustine*, __ N.E.3d __, 467 Mass. 230, 245 (2014) (noting that "the cellular telephone has become an indispensable part of modern American life") (citations and internal quotation marks omitted); *State v. Earls*, 70 A.3d 630, 643 (N.J. 2013) (same). *See also United States v. Jones*, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (noting that, as of June, 2011, "there were more than 322 million wireless devices in use in the United States"). This factor "strengthen[s] the case" for a greater expectation of privacy and recognition that society views that expectation as

[10] Notably, landline use has markedly declined in the United States, with an increasing number of American households relying exclusively on cell phones. During the first half of 2013, 39.4% of American households were cell-phone only (i.e., having no landline but at least one cell phone). *See* STEPHEN J. BLUMBERG & JULIAN V. LUKE, NAT'L CTR. FOR HEALTH STATISTICS, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JANUARY–JUNE 2013, at 1 (Dec. 2013), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201312.pdf.

reasonable. *Quon*, 560 U.S. at 760; *see also Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

B. The Third-Party Doctrine and *Smith v. Maryland* Are Inapposite

The district court concluded that the Fourth Amendment is not applicable to the NSA's collection of telephony metadata based on the so-called third-party doctrine. The third-party doctrine provides that information "knowingly exposed" to a third party is not protected by the Fourth Amendment because one "assumes the risk" that the third party will disclose that information to the government.[11]

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the Fourth Amendment was not implicated when defendant's telephone company, at the request of the police, placed a "pen register" on the defendant's phone in order to track the telephone numbers called from that phone. *Smith*, 442 U.S. at 744-46. In reaching this decision, the Court explained that, since a person knowingly exposes phone numbers to the phone company when dialing (to enable the phone company to connect him) and realizes that any numbers he calls may be monitored for billing purposes, the Fourth Amendment does not protect the privacy of those numbers. *Id.* at 744-45.

[11] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 527 (2006).

The facts and circumstances of *Smith* differ so markedly from those at issue here that the *Smith* holding cannot determine the legality of the NSA metadata program. In *Smith*, police had information strongly indicating that a man who had burglarized a home was calling its occupant and harassing her. At their request, the telephone company installed a pen register to record the numbers dialed from the suspect's telephone, looking for one number in particular. *Id.* at 737. The use of the pen register was therefore specific in purpose, limited in duration (one to three days), and focused exclusively on an individual that the police reasonably suspected of criminal activity.

The NSA's phone metadata program, by contrast, involves mass surveillance—equivalent to placing on every phone in the United States a pen register that is susceptible to advanced processing, including network analysis and data mining. This surveillance, which is ongoing and continuous over a period of years, is unsupported by any suspicion that the mass-targeted individuals are engaged in any wrongdoing. Indeed, the government has acknowledged that almost all of the information thus obtained will bear no relationship whatsoever to criminal activity.[12]

---

[12] *See* Order, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13, 2009 WL 9150913, at *11-12 (FISA Ct. Mar. 2, 2009) ("The government's applications have all acknowledged that, of the [REDACTED] of call detail records NSA receives per day (currently over [REDACTED] per day), the vast majority of individual records that are being sought pertain neither to [REDACTED]. . . In other words, nearly all of the call detail records collected pertain to communications of non-U.S. persons who are not the subject of an FBI investigation to obtain foreign intelligence information, are communications of U.S. persons who are not the subject of an FBI investigation to protect against international terrorism or clandestine intelligence activities.").

The limited use of a pen register (trap-and-trace device)[13] 35 years ago in *Smith*—against a single individual and for a period of two/three days—did not threaten individual privacy in the way that the systematic, indiscriminate collection and aggregation of large datasets do. "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010). In *United States v. Jones*, 132 S. Ct. 945 (2012), five Supreme Court Justices agreed that, when the government engages in prolonged GPS location tracking, it conducts a search under the Fourth Amendment. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and, indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period"); *id.* at 955 (Sotomayor, J., concurring) ("[M]aking available . . . such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society." (internal quotation marks omitted)); *id.* (stating that individuals have "a reasonable societal expectation of privacy in the sum of [their] public movements").

[13] Traditionally, a pen register records the telephone numbers called by the subject telephone while the trap-and-trace device gathers the incoming telephone numbers.

Dragnet surveillance of this nature can yield troves of information about vast numbers of innocent individuals: intimate relationships, political affiliations, everyday habits, medical/psychological treatments, legal counsel, business decisions, political affiliations, and more. *Cf. United States v. Knotts*, 460 U.S. 276, 284-85 (1983) (reserving question of whether the Fourth Amendment would treat dragnet location tracking differently from location tracking of a single individual). Calls to a rape-crisis line, an abortion clinic, a suicide hotline, or a political party headquarters reveal significantly more information than what was being sought in *Smith*.

Even if the NSA examines only a small fraction of the immense amount of information it collects, the Fourth Amendment is implicated simply by the government's *collection and acquisition* of information, regardless of whether the government subsequently uses that information. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("[A] violation of the [Fourth] Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion." (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974))); *accord Soldal v. Cook Cnty.*, 506 U.S. 56, 67 n.11 (1992). The NSA cannot immunize this dragnet surveillance program from Fourth Amendment scrutiny by its simple assurance that the American people's private information will be safe in its hands.

Most importantly, significant technological and societal changes mean that the level of intrusion and the resulting harm to U.S. citizens' privacy interests are fundamentally different from the situation that the Court confronted in 1979. In

Smith, the Court relied heavily on the fact that, when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." *Smith*, 442 U.S. at 744. Unlike the phone numbers dialed in *Smith*, metadata is neither tangible nor visible to a user. When users switch on their cell phone (most mobile phones remain "on" virtually all the time, even in "sleep" and "airplane" mode) and make a call, for example, they are not required to enter their zip code, area code, or any other location identifier. Nor do the digits they press in making the call reveal their own location. Rather, phone metadata (including location data) is created and transmitted *automatically* to the network provider's computers—entirely independent of the user's input, control, knowledge, or volition. Thus, unlike *Smith*, where the information at issue was unquestionably conveyed by the defendant to a third party, persons monitored under the NSA's program would have no reason to expect that metadata about their calls (including geographic location)—automatically generated and conveyed to the telecommunications provider—would be exposed to anyone.

Moreover, the metadata collected under the NSA's program conveys far more information than the pen register in *Smith*. Trunk information, nonexistent in 1979, reveals not just the target of a particular phone call, but where the callers (and receivers) are located. At the time *Smith* was decided, the police could determine only when someone was located at Smith's home. The telephone did not follow Smith around. By contrast, mobile technologies now allow the police to ascertain where persons are located, creating a second layer of surveillance based simply on trunk

identifier information. *See Earls*, 70 A.3d at 642 (N.J. 2013) ("Modern cell phones also blur the historical distinction between public and private areas because cell phones emit signals from both places."). The bulk collection of records, then, means that the government has the ability to monitor the movement of not just one individual but nearly the entire American citizenry. As the district court noted in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), "The question . . . [in this case] is *not* the same question that the Supreme Court confronted in *Smith*. To say the least, whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment—under the circumstances addressed and contemplated in [*Smith*]—is a far cry from the issue in this case." *Klayman*, 957 F. Supp. 2d at 31 (citations and internal quotation marks omitted).

The assumption-of-risk theory espoused by *Smith* necessarily entails a knowing or voluntary act of disclosure that is simply not present in the NSA metadata dragnet.[14] The premise that all U.S. citizens have voluntarily conveyed information about every call they have made or received over a period of years, and knowingly made that information available for collection by the government, is a fiction that

[14] Although the *Smith* Court found automation irrelevant and was "[dis]inclined to hold that a different constitutional result is required because the telephone company has decided to automate," *Smith*, 442 U.S. at 744-45, the Court has also repeatedly tied the question of whether government action constitutes a search to whether it invades a reasonable expectation of privacy, *see, e.g.*, *United States v. Jones*, 132 S. Ct. 945, 950-51 (2012); *Bond v. United States*, 529 U.S. 334, 337-39 (2000); *California v. Ciraolo*, 476 U.S. 207, 213-14 (1986); *Katz*, 389 U.S. at 360. And research reveals that Internet users do in fact "sharply distinguish between disclosure to humans and disclosure to automated systems, even if courts thus far have not." Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 586-87, 628 (2011).

effectively insulates a mass surveillance program from Fourth Amendment scrutiny. *See In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 126-27 (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."). Fourth Amendment protections are not ceded by the unknowing, inadvertent, and computer-generated disclosure of metadata.

1. Phone Metadata Can Reveal Highly Personal Information

Security experts agree that metadata can reveal just as much intimate information about an individual as the contents of her communication and provide a map of associations throughout the country and the world.[15] Michael Morrell, surveillance task force member and former deputy CIA director, challenged the content-metadata dichotomy before the Senate Judicial Committee in January 2014 and acknowledged that phone metadata inherently entails substantive details about the

[15] Two separate committees assembled by the executive branch—the President's Review Group on Intelligence and Communications Technology, and the Privacy and Civil Liberties Oversight Board—have both recognized the need to reevaluate the content-metadata distinction. *See, e.g.*, PRESIDENT'S REVIEW GROUP, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP IN INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (Dec. 12, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (calling for an end to the metadata collection program and making dozens of recommendations for significant reforms); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 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 10 (Jan. 23, 2014), http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (calling for an end to the metadata collection program based on statutory and constitutional concerns).

communication: "There is *quite a bit of content in metadata* . . . . There's not a sharp distinction between metadata and content. It's more of a continuum."[16] Cryptology and security expert Matt Blaze explains,

> Metadata is our context. And that can reveal far more about us—both individually and as groups—than the words we speak. Context yields insights into who we are and the implicit, hidden relationships between us. A complete set of all the calling records for an entire country is therefore a record not just of how the phone is used, but, coupled with powerful software, of our importance to each other, our interests, values, and the various roles we play.[17]

Simply put, "*metadata is often a proxy for content*." Felten Declaration ¶ 39 (emphasis added) (footnote citation omitted).

In *Smith*, the Supreme Court also assessed the degree of invasiveness of the particular surveillance to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," explaining that "'a law enforcement official could not even determine from the use of a pen register whether a communication existed.'" *Smith*, 442 U.S. at 741, 742 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)). Aggregate metadata can, as noted above, reveal vastly more. Aggregation "allows the government to construct social graphs and to study their evolution and communications patterns over days, weeks, months, even years." Felten Declaration ¶ 58. And even a small collection can expose a great

---

[16] *See* Spencer Ackerman, *NSA Review Panel Casts Doubt on Bulk Data Collection Claims*, GUARDIAN (Jan. 14, 2014), http://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism (emphasis added).

[17] Matt Blaze, *Phew, NSA Is Just Collecting Metadata (You Should Still Worry)*, WIRED (June 19, 2013), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again/.

deal. For example, if one calls a gynecologist, then calls an oncologist, and then a family member, the person who reviews that record will likely have a very good guess as to what those calls were about. "Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant." Felten Declaration ¶ 58.[18] By collecting and analyzing huge amounts of data, often of different types, government actors can extract even more, including facts that individuals consciously choose not to reveal and even patterns that they may not recognize about themselves.

Aggregation figured prominently in the *Jones* Court's conclusion that long-term, warrantless GPS surveillance amounted to a search. Five members of the Court

[18] In recent years, the government has effectively used primary telephone data, as distinct even from metadata, as proof of criminal activity. For example, in a string of successful SDNY insider-trading prosecutions, *subpoenaed* phone records—showing the likely identities of the caller and the party called, the time of the call, and the call duration—along with trading records, provided circumstantial evidence of insider trading. *See, e.g.*, *United States v. Rajaratnam*, 802 F. Supp. 2d 491, 502-05 (S.D.N.Y. 2011) (jury finding of conspiracy to commit insider trading was supported by sufficient evidence, including telephone records showing tippee had called defendant around the time the tips were conveyed; records of instant messages between tippee and defendant directing defendant to wait until she had a tip to trade; and trading records showing that, shortly after the calls, both defendant and tippee had traded the securities at issue); *United States v. McDermott*, 245 F.3d 133, 138-39 (2d Cir. 2001) (circumstantial evidence that phone conversations between investment banker and his girlfriend coincided with 21 successful stock trades made by girlfriend, that many of trades were in stocks of banks subject to non-public negotiations with banker's firm, and that girlfriend shared information with her associate, was sufficient to convict defendant of insider trading, notwithstanding lack of direct evidence of the phone conversations' contents). There can be no doubt that properly acquired telephone data can be an enormously effective law enforcement tool. Likewise, dragnet, indiscriminate acquisition of data can be an even more powerful tool. But at what cost?

distinguished traditional law enforcement methods from long-term GPS surveillance. Justices Alito and Sotomayor each wrote concurring opinions that recognized the privacy concerns implicated by data aggregation.

In a concurrence joined by Justices Breyer, Kagan, and Ginsburg, Justice Alito reasoned,

> [R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.

Jones, 132 S. Ct. at 964 (Alito, J., concurring).

Justice Sotomayor observed that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and that the "Government can store such records and efficiently mine them for information years into the future." *Id.* at 956 (Sotomayor, J., concurring). Discussing the third-party doctrine, she said, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and

so on." *Id.* at 956.[19] *See also Whalen v. Roe*, 429 U.S. 589, 606 (1977) ("We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . ."). In sum, the collection and aggregation of phone metadata allows the government access to sensitive information in a way that would otherwise be unlawful without a court-authorized search of an individual's records.

2. Under *United States v. Jones*, a Person Does Not Forfeit His Constitutionally Protected Privacy Interest in Information Simply Because It Is Accumulated on a Telecommunications Provider's Computers.

The Supreme Court has never held that the government is free to collect any and all information that may wind up in computer data bases as a result of common, everyday activities, such as making telephone calls or traveling around in one's car. To the contrary, in *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court considered long-term recording and aggregation of location information from a GPS device that police warrantlessly installed on a suspect's car. The government had

[19] The Supreme Court has also highlighted the privacy concerns at stake in other constitutional and statutory contexts. For example, in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), the Supreme Court held that Freedom of Information Act (FOIA) exemption 7(c) prohibited disclosure of FBI "rap sheets" to the media even though they were compiled entirely from information already in public records. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 762-71. In reaching that result, the Court focused on the expanding capacity of database technology to aggregate and store mass quantities of personal data. Thus, the Court saw "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations . . . and a computerized summary located in a single clearinghouse of information." *Id.* at 763. The privacy interest in criminal rap sheets was deemed "substantial" under FOIA because "in today's society, the computer can accumulate and store information" to such an extent and degree that it violates a "privacy interest in maintaining the practical obscurity" of that information. *Id.* at 771, 780.

argued that use of the device was not a search because it revealed only information the defendant already disclosed to others—the location of his vehicle on the public roads.

In *Jones*, five Justices raised concerns about the government's technological capacity to gather data revealing personal details about our lives. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring). *Jones* is only the most recent of a line of Supreme Court decisions reflecting the principle that third-party access to information alone does not waive an individual's Fourth Amendment rights. *See, e.g.*, *Kyllo*, 533 U.S. at 40 (thermal signatures emanating from a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff); *Bond v. United States*, 529 U.S. 334, 338-39 (2000) (personal luggage in overhead bin on bus). In these cases, the Court made clear that the mere fact that a person has shared information with a third party does not extinguish that person's constitutionally protected privacy interest in it. *See also United States v. Warshak*, 631 F.3d 266, 284-86 (6th Cir. 2010) (finding reasonable expectation of privacy in the email defendant had stored with an ISP).

Similarly, in other Fourth Amendment contexts, access to a protected area for one limited purpose does not render that area suddenly unprotected from government searches. *See, e.g.*, *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009) (tenants have reasonable expectation of privacy in their apartments even though landlords have a right to enter); *United States v. Stevenson*, 396 F.3d 538, 546 (4th Cir. 2005) ("And

the protection of a house extends to apartments, rented rooms within a house, and hotel rooms so that a landlord may not give the police consent to a warrantless search of a rented apartment or room."); *United States v. Paige*, 136 F.3d 1012, 1020 n.1 (5th Cir. 1998) ("[A] homeowner's legitimate and significant privacy expectation . . . cannot be entirely frustrated simply because, ipso facto, a private party (e.g., an exterminator, a carpet cleaner, or a roofer) views some of these possessions.").

C. The Third-Party Doctrine Is Inapplicable to the NSA's Collection, Retention, and Aggregation of Nationwide Computer-Generated Phone Metadata.

The third-party doctrine has been widely criticized by legal scholars[20] and repudiated by several states under their respective constitutions.[21] *See Kyllo*, 533 U.S. at

[20] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007) (explaining the normative and descriptive flaws inherent in the acquisition of information through the third-party doctrine); 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(b), (c) (5th ed. 2012) (commenting that the decisions applying the third-party doctrine are "dead wrong" and "make[] a mockery of the Fourth Amendment"); Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. U. L. REV. 1, 21-28 (1983); Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 245-65 (2006) (arguing that the third-party-doctrine cases were wrongly decided on several grounds); Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After* Lawrence, 57 UCLA L. REV. 1 (2009); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1097-1108 (2006); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 40-50, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf; JoAnn Guzik, Comment, *The Assumption of Risk Doctrine: Erosion of Fourth Amendment Protection Through Fictitious Consent to Search and Seizure*, 22 SANTA CLARA L. REV. 1051, 1068-72 (1982); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 981-85 (2007) (arguing that information placed in the hands of a third party should still be entitled to a reasonable expectation of privacy); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 564-66 (1990); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. &

34 (internal quotation and citation omitted). In light of dramatic developments in technology, the third-party doctrine should evolve to preserve reasonable expectation of privacy in the modern world so that the Fourth Amendment does not, as in Justice Sotomayor's words, "treat secrecy as a prerequisite for privacy," *Jones*, 132 S. Ct. at 957. *See Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." (citing *Kyllo*, 533 U.S. at 34)). As Justice Marshall noted in *Smith*, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have

---

TECH. 2, ¶ 5 (advocating a "retooling" of the third-party doctrine for internet searches); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1254-56 (1983) (arguing that the third-party doctrine cases are incorrect because they focus on the rights of the guilty rather than the rights of the innocent); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113 (2008) (arguing that the "Stranger Principle [underlying the third-party doctrine] is completely untenable"); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) (the third-party doctrine "presents one of the most serious threats to privacy in the digital age"); Scott E. Sundby, "*Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757-58 (1994).

[21] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 (2006) (listing California, Colorado, Florida, Hawaii, Idaho, Illinois, Montana, New Jersey, and Pennsylvania as states that have rejected the federal third-party doctrine); *Commonwealth v. Augustine*, __ N.E.3d __, 467 Mass. 230, 245-46 (2014) (under Massachusetts constitution, third-party doctrine did not apply in determining whether defendant had a reasonable expectation of privacy in cellular site location information (CSLI) because defendant never voluntarily conveyed CSLI to his service provider; the information was unknown and unknowable to defendant in advance.). *See, e.g.*, *State v. Walton*, No. SCWC-11-00667, __ P.2d __, 2014 WL 594105, at *32 (Haw. Feb. 14, 2014) (rejecting the third party doctrine as inconsistent with the Hawaii constitution and noting that an individual may "retain a legitimate expectation that . . . information [shared with a third party] will not be further disseminated for purposes other than those for which they were disclosed in the first place"); *Burrows v. Super. Court*, 529 P.2d 590, 593 (Cal. 1974) (under California constitution, defendant had reasonable expectation of privacy in his bank records); *People v. Oates*, 698 P.2d 811, 815-18 (Colo. 1985) (en banc) (rejecting the third-party doctrine as it applies to electronic tracking); *People v. Corr*, 682 P.2d 20, 26-27 (Colo. 1984) (en banc) (finding, under Colorado constitution, reasonable expectation of privacy in phone numbers dialed).

no realistic alternative." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).[22] Phone users have no recourse to prevent the collection of metadata; "it can only be avoided at the price of not using a . . . phone." *See State v. Earls*, 70 A.3d 630, 641 (2013). Given "the vital role that the . . . phone"—particularly, the cell phone—"has come to play in private communication," *see Katz*, 389 U.S. at 352, this is not a viable option. *See In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 126-27 (E.D.N.Y. 2011).

The impact of bulk metadata collection on lawyers and physicians illustrates the broader threat this collection poses. Lawyers speak with clients by phone far more often than in person. The NSA is, by the government's admission, collecting the metadata of those phone calls. Physicians speak with patients by phone regularly. Likewise, the NSA's program gathers the metadata of those calls. Lawyers—who are under an ethical obligation to preserve client confidences and who know that

---

[22] *See also* Scott E. Sundby, "*Everyman*"*'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1789-90 (1994) ("To maintain privacy, one must not write any checks nor make any phone calls. It would be unwise to engage in conversation with any other person, or to walk, even on private property, outside one's house . . . . The wise individual might also consider purchasing anti-aerial spying devices if available . . . . Upon retiring inside, be sure to pull the shades together tightly so that no crack exists and to converse only in quiet tones. When discarding letters or other delicate materials, do so only after a thorough shredding of the documents."); Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made Of?*, 41 U.C. DAVIS L. REV. 781, 799 (2008) ("[T]he reasonably private person must be a super-paranoid individual who has walled in his house, speaks in code, buries the trash in the backyard, and keeps money under the mattress"); Elizabeth Paton-Simpson, *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places*, 50 U. TORONTO L.J. 305, 305-06 (2000) (describing an "entirely reasonable" character named Prudence who "could be accused of being paranoid" because she "refuses to chat with friends over the telephone," "develops all her photographs herself," and takes various other steps to "avoid being judged to have given implied consent to surveillance [of her conduct]").

disclosure to third-parties can obviate attorney-client privilege—should not have to hesitate to call clients or answer the phone out of fear that doing so will vitiate privileges or expose the client's confidential information. Physicians, too, are sensitive to their patients' privacy. Yet no physician hesitates to inform of test results by telephone for fear of breaching a confidence. Although we live in a world of targeted online advertising based on past computer usage, we should be able to remain confident that the Fourth Amendment acts as a buffer between what Google's and Amazon's computers know and what the government knows.

The data gathered by the computers of Verizon, AT&T, and any other telecommunication companies are not, in any meaningful sense, ceded by customers knowingly and voluntarily. In the same way that a lawyer does not hesitate to speak on a telephone with a client, or a physician with a patient, for fear of a third-party disclosure, no one hesitates to make or receive a telephone call for fear that doing so will thereby authorize the government to mine the calls' metadata because the data has been provided to a third party in the form of an enormous computer array maintained by Verizon, AT&T, or their competitors.

CONCLUSION

The Association submits that the standards and protections of the Fourth Amendment to the Constitution should apply to the NSA's bulk telephony metadata collection program. Because the district court erroneously concluded that the

program is not a "search" and is therefore outside the protection of the Fourth Amendment, the decision below should be reversed.

Dated: New York, NY
March 13, 2014

Respectfully submitted,

/s/ Gary D. Sesser

Jonathan Hafetz
Chair, Task Force on National Security
and the Rule of Law
ASSOCIATION OF THE BAR
OF THE CITY OF NEW YORK
42 West 44th Street
New York, NY 10036
Tel.: (212) 382-6600

Gary D. Sesser
Stephen L. Kass
Michael Shapiro
Laura A. Zaccone
CARTER LEDYARD & MILBURN LLP
Two Wall Street
New York, NY 10005
Tel.: (212) 732-3200
Fax: (212) 732-3232

Counsel for the Association of the Bar of the City of New York

CERTIFICATE OF COMPLIANCE

I hereby certify that the attached brief complies with the type-volume limitation provided in Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure. The brief contains 7,380 words of Garamond proportional typeface (14-point in the body of the brief and 12-point in the footnotes). Microsoft Word is the word-processing software that was used to prepare the brief.

Dated: New York, New York
March 13, 2014

/s/ Gary D. Sesser

Gary D. Sesser
Stephen L. Kass
Michael Shapiro
Laura A. Zaccone
CARTER LEDYARD & MILBURN LLP
Two Wall Street
New York, NY 10005
Tel.: (212) 732-3200
Fax: (212) 732-3232