14-42

IN THE

United States Court of Appeals
for the Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES ii

INTEREST OF AMICUS CURIAE 1

PRELIMINARY STATEMENT 3

ARGUMENT 5

I. The NSA's Mass Collection of Phone Metadata Is a Search Under the Fourth Amendment. 5

A. The ACLU Subjectively Expected That Its Phone Metadata Would Remain Private and That Expectation Was Objectively Reasonable. 6

B. The Third-Party Doctrine and *Smith v. Maryland* Are Inapposite 9

1. Phone Metadata Can Reveal Highly Personal Information 15

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. 19

C. The Third-Party Doctrine Is Inapplicable to the NSA's Collection, Retention, and Aggregation of Nationwide Computer-Generated Phone Metadata 21

TABLE OF AUTHORITIES

Page(s)

Cases

Am. Civil Liberties Union v. Clapper,
No. 13-cv-03994 (WHP), slip op. (S.D.N.Y. Dec. 27, 2013) 2, 3

Bond v. United States,
529 U.S. 334 (2000) 14, 20

Burrows v. Super. Court,
529 P.2d 590 (Cal. 1974) 22

California v. Ciraolo,
476 U.S. 207 (1986) 14

City of Ontario, Cal. v. Quon,
560 U.S. 746 (2010) 7, 8

Commonwealth v. Augustine,
__ N.E.3d __, 467 Mass. 230 (2014) 8, 22

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

Georgia v. Randolph,
547 U.S. 103 (2006) 8

In re Production of Tangible Things from [Redacted],
No. BR 08-13, 2009 WL 9150913 (FISA Ct. Mar. 2, 2009) 4, 10

In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.,
809 F. Supp. 2d 113 (E.D.N.Y. 2011) 15, 23

Katz v. United States,
389 U.S. 347 (1967) 5, 6, 14, 23

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013) 4, 14

Kyllo v. United States,
533 U.S. 27 (2001) 8, 9, 20, 21, 22

People v. Corr,
682 P.2d 20 (Colo. 1984) 22

People v. Oates,
698 P.2d 811 (Colo. 1985) 22

Smith v. Maryland,
442 U.S. 735 (1979) .....passim

Soldal v. Cook Cnty.,
506 U.S. 56 (1992)..... 12

Spectrum Sys. Int'l Corp. v. Chem. Bank,
581 N.E.2d 1055 (N.Y. 1991) 2

State v. Earls,

United States v. Paige,
136 F.3d 1012 (5th Cir. 1998)..... 21

United States v. Rajaratnam,
802 F. Supp. 2d 491 (S.D.N.Y. 2011)..... 17

United States v. Stevenson,
396 F.3d 538 (4th Cir. 2005)..... 21

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990) 12

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010)..... 20, 22

United States v. Washington,
573 F.3d 279 (6th Cir. 2009)..... 20

Whalen v. Roe,
429 U.S. 589 (1977) 19

Constitutional Provisions

U.S. CONST. amend. IV .....passim

Statutes and Rules

50 U.S.C. § 1861..... 3

FED. R. APP. P. 29(c)(5)..... 1

FED. R. APP. P. 32(a)(7)(B) 26

Local Rule of the Court of Appeals for the Seco9.36 -2222-2.6 -222 C(eair36 -222cui-2.00671)2.13

Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*,
4 N. ILL. U. L. REV. 1 (1983) 21

Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289 (1981) 21

Matt Blaze, *Phew, NSA Is Just Collecting Metadata (You Should Sthh 4T f6T d[()5)2M(S)4Vualle.....hdi(3)05(l)*

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. & TECH. 1 21

Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983) 22

Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009) 22

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 6

Elizabeth Paton-Simpson, *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places*, 50 U. TORONTO L.J. 305 (2000) 23

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 2

Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (2008) 22

Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) 9

Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005) 22

Scott E. Sundby, "*Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751 (1994) 22, 23

.

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]

action—need not be subverted during times of war or other crises. It believes that

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

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

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 it999(a)-67036002994(e)7.991≥2.99.04 T

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").

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

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

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

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 der

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*

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

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*

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

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 Protecti*[illegible]

no realistic alternative." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).[22] Phone users hav

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