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,

– v. –

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 PLAINTIFFS-APPELLANTS

Christopher T. Dunn
Arthur N. Eisenburg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

Jameel Jaffer
Alex Abdo
Patrick Toomey
Brett Max Kaufman
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

RULE 26.1 CORPORATE DISCLOSURE STATEMENT

Plaintiffs–Appellants are affiliated non-profit membership corporations. They have no stock and no parent corporations, and no corporation owns more than 10% of their stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES iv

INTRODUCTION 1

JURISDICTIONAL STATEMENT 3

ISSUES PRESENTED FOR REVIEW 4

STATEMENT OF THE CASE 5

STATEMENT OF FACTS & PROCEDURAL HISTORY 6

SUMMARY OF THE ARGUMENT 15

STANDARD OF REVIEW 16

ARGUMENT 17

I. The district court erred in holding that the phone-records program is authorized by statute 17

A. Section 215 does not authorize the government to collect phone records 17

B. Even if Section 215 authorizes the government to collect phone records, it does not authorize it to collect phone records on this scale 21

C. Congress did not ratify the phone-records program when it reauthorized Section 215 in 2010 and 2011 26

II. The district court erred in holding that Plaintiffs' statutory claims are impliedly precluded 29

A. Plaintiffs' statutory claim is not precluded by 18 U.S.C. § 2712 30

B. Plaintiffs' statutory claim is not precluded by Section 215 31

III. The program violates the Fourth Amendment 38

A. The government's bulk collection of phone records constitutes a search under the Fourth Amendment 38

B. The government's bulk collection of telephony metadata is unreasonable.....46

1. The phone-records program involves warrantless searches, which are per se unreasonable.....46

2. The government's bulk collection of telephony metadata is unreasonable 48

IV. The program violates the First Amendment 53

A. The program substantially burdens Plaintiffs' First Amendment rights 53

B. The phone-records program fails "exacting scrutiny" because it is unduly broad 58

V. The district court erred in denying Plaintiffs' motion for a preliminary injunction.....60

CONCLUSION 62

TABLE OF AUTHORITIES

Page(s)

Cases

Absolute Activist Value Master Fund Ltd. v. Ficeto, 677 F.3d 60 (2d Cir. 2012) 16

ACLU v. Ashcroft, 322 F.3d 240 (3d Cir. 2003) 61

ACLU v. Clapper, No. 1:13-cv-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) 5

Ark. Dairy Coop. Ass'n v. U.S. Dep't of Agric., 573 F.3d 815 (D.C. Cir. 2009) 37

Atkins v. Parker, 472 U.S. 115 (1985) 26

Berger v. New York, 388 U.S. 41 (1967) 46, 48, 49

Biddle v. Comm'r of Internal Revenue, 302 U.S. 573 (1938) 26

Block v. Community Nutrition Institute, 467 U.S. 340 (1984) 34, 35, 36

Bond v. United States, 529 U.S. 334 (2000) 45

Bowen v. Mich. Acad. of Family Practices, 476 U.S. 667 (1986) 29

Bowman Dairy Co. v. United States, 341 U.S. 214 (1951) 23

Brigham City v. Stuart, 547 U.S. 398 (2006) 48

Buckley v. Valeo, 424 U.S. 1 (1976) 53

Bursey v. United States, 466 F.2d 1059 (9th Cir. 1972) 59

Carroll v. United States, 267 U.S. 132 (1925) 47

Chandler v. Miller, 520 U.S. 305 (1997) 50

Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd., 598 F.3d 30 (2d Cir. 2010) 60

City of Indianapolis v. Edmond, 531 U.S. 32 (2000) 47

Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013)..... 12, 57

Clark v. Library of Cong., 750 F.2d 89 (D.C. Cir. 1984).....53

Clark v. Martinez, 543 U.S. 371 (2005) 38

Cohen v. United States, 650 F.3d 717 (D.C. Cir. 2011) 29

Comm'r of Internal Revenue v. Glenshaw Glass Co., 348 U.S. 426 (1955).....29

Council for Urological Interests v. Sebelius, 668 F.3d 704 (D.C. Cir. 2011) 37

Covino v. Patrissi, 967 F.2d 73 (2d Cir. 1992).....60

Demarest v. Manspeaker, 498 U.S. 184 (1991) 21

Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) 32

Ealy v. Littlejohn, 569 F.2d 219 (5th Cir. 1978).....54

FEC v. LaRouche Campaign, 817 F.2d 233 (2d Cir. 1987) 56

Ferguson v. City of Charleston, 532 U.S. 67 (2001)..... 45, 47

Florida v. Jardines, 133 S. Ct. 1409 (2013).....45

Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539 (1963)..... 55, 56

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573 (FISC Aug. 29, 2013) 10, 37

In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 (FISC Oct. 11, 2013) 10

In re Grand Jury Proceedings, 776 F.2d 1099 (2d Cir. 1985) 53

In re Grand Jury Proceedings, 863 F.2d 667 (9th Cir. 1988) 59

In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11 (S.D.N.Y. 1994) 23

In re Grand Jury Subpoena, 701 F.2d 115 (10th Cir. 1983) 59

In re Horowitz, 482 F.2d 72 (2d Cir. 1973) 23

In re Sealed Case, 310 F.3d 717 (FISCR 2002) 50

In re Six Grand Jury Witnesses, 979 F.2d 939 (2d Cir. 1992) 23

In re Stoltz, 315 F.3d 80 (2d Cir. 2002) 18

Katz v. United States, 389 U.S. 347 (1967) 42, 46

Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) 12, 40

Koretoff v. Vilsack, 614 F.3d 532 (D.C. Cir. 2010) 37

Kyllo v. United States, 533 U.S. 27 (2001) 38

Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267 (2d Cir. 1981) 54, 55, 57, 58

Memphis Planned Parenthood, Inc. v. Sundquist, 175 F.3d 456 (6th Cir. 1999) 61

Michigan v. U.S. Army Corps of Engineers, 667 F.3d 765 (7th Cir. 2011) 35

Missouri v. McNeely, 133 S. Ct. 1552 (2013) 48

Mitchell v. Cuomo, 748 F.2d 804 (2d Cir. 1984) 60

Moore v. Obama, No. 09-5072, 2009 WL 2762827 (D.C. Cir. Aug. 24, 2009) 45

Mullins v. City of N.Y., 634 F. Supp. 2d 373 (S.D.N.Y. 2009) 61

Natural Res. Def. Council v. Johnson, 461 F.3d 164 (2d Cir. 2006) 30

New Jersey v. T.L.O., 469 U.S. 325 (1985) 47

Paton v. La Prade, 469 F. Supp. 773 (D.N.J. 1978).....56

Sackett v. EPA, 132 S. Ct. 1367 (2012) 29, 34

Samson v. California, 547 U.S. 843 (2006).....49

Shelton v. Tucker, 364 U.S. 479 (1960)..... 56, 57, 59

Smith v. Maryland, 442 U.S. 735 (1979) 39

Soldal v. Cook Cnty., 506 U.S. 56 (1992).....44

Statharos v. N.Y. City Taxi & Limousine Comm'n, 198 F.3d 317 (2d Cir. 1999) 60

Tabbaa v. Chertoff, 509 F.3d 89 (2d Cir. 2007) 55

United States v. Barbera, 514 F.2d 294 (2d Cir. 1975).....47

United States v. Cafero, 473 F.2d 489 (3d Cir. 1973) 50

United States v. Calamaro, 354 U.S. 351 (1957) 28

United States v. Citizens Bank, 612 F.2d 1091 (8th Cir. 1980).....59

United States v. Duggan, 743 F.2d 59 (2d Cir. 1984) 50

United States v. Epstein, 620 F.3d 76 (2d Cir. 2010) 21

United States v. Head, 416 F. Supp. 840 (S.D.N.Y. 1976) 60

United States v. Jones, 132 S. Ct. 945 (2012) 41, 42, 43, 45

United States v. Karo, 468 U.S. 705 (1984) 46

United States v. Knoll, 16 F.3d 1313 (2d Cir. 1994) 45

United States v. Knotts, 460 U.S. 276 (1983)..... 40, 41

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).....41

United States v. Ramsey, 431 U.S. 606 (1977) 55

United States v. Smith, 499 U.S. 160 (1991) 18

United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973).....50

United States v. U.S. District Court (*Keith*), 407 U.S. 297 (1972) 6, 47

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) 44

Virginia v. Moore, 553 U.S. 164 (2008).....49

Whitman v. Am. Trucking Ass'ns, Inc., 531 U.S. 457 (2001).....25

Zervos v. Verizon N.Y., Inc., 252 F.3d 163 (2d Cir. 2001) 17

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 55

Statutes

5 U.S.C. § 702 .....3, 29

18 U.S.C. § 2702 17

18 U.S.C. § 2703 ..... 17, 51

18 U.S.C. § 2708 35

18 U.S.C. § 2709 ..... 20, 24, 32, 51

18 U.S.C. § 2712 ..... 30, 31

18 U.S.C. § 3122 51

18 U.S.C. § 3125 51

18 U.S.C. § 3511 32

20 U.S.C. § 1232 24

28 U.S.C. § 1291 3

28 U.S.C. § 1331 3

38 U.S.C. § 4326 25

50 U.S.C. § 1801 6

50 U.S.C. § 1803 6

50 U.S.C. § 1806 31

50 U.S.C. § 1822 20

50 U.S.C. § 1825 31

50 U.S.C. § 1842 ..... 20, 21, 51

50 U.S.C. § 1845 31

50 U.S.C. § 1861 ..... passim

50 U.S.C. § 1862 7

50 U.S.C. § 1881 20

USA PATRIOT Act of 2001, Pub. L. 107-56 7

Other Authorities

124 Cong. Rec. 34 (1978) 36

157 Cong. Rec. S3386 (daily ed. May 26, 2011) (statement of Sen. Ron Wyden) 8

157 Cong. Rec. S3389 (daily ed. May 26, 2011) (statement of Sen. Mark Udall) 8

Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act (Aug. 9, 2013) 9, 51

Br. *Amicus Curiae* of Congressman F. James Sensenbrenner, Jr. in Supp. of Pls., *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Sept. 4, 2013), ECF No. 46-1 26

Br. of *Amici Curiae* U.S. Representatives Amash et al., *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (FISC June 28, 2013).....28

Defendants' Mem. of Law in Supp. of Mot. to Dismiss 24, *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Aug. 26, 2013).....22

Defs.' Mem. of Law in Opp. to Pls.' Mot. for a Preliminary Injunction, *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Oct. 1, 2013), ECF No. 66.....25

Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, Daily Beast, Feb. 17, 2014.....34

Glen Kessler, *James Clapper's "Least Untruthful" Statement to the Senate*, Wash. Post, June 12, 2013.....8

H.R. Rep. 109-174, pt. 1 (2005).....32

Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary, 109th Cong. (2005) (testimony of Kenneth Wainstein, U.S. Att'y for the District of Columbia).....33

James R. Clapper, Director of National Intelligence, *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal. Dec. 20, 2013), ECF No. 168.....8

Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013.....48

Letter from Ronald Weich, Assistant Attorney General, to Hon. Nydia Velázquez, Chair, Congressional Hispanic Caucus, U.S. House of Representatives (Mar. 3, 2010).....19

Letter from Sen. Ron Wyden & Sen. Mark Udall to Eric Holder, Att'y Gen. (Sept. 21, 2011).....28

Morgan Cloud, *Searching Through History; Searching For History*, 63 U. Chi. L. Rev. 1707 (1996).....46

Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013) 38

Office of Legal Counsel, Memorandum Opinion for the General Counsel [of the] FBI: Requests for Information Under the Electronic Communications Privacy Act (Nov. 5, 2008) 18

Office of the Inspector General, A Review of the FBI's Use of Section 215 Orders for Business Records (2007) 19

Order Granting the Government's Motion to Amend the Court's Primary Order Dated January 3, 2014, No. BR 14-01 (FISC Feb. 5, 2014) 15

Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06-05 (FISC May 24, 2006) 9

Order, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13 (Mar. 2, 2009) 51

Peter Wallsten, *House Panel Withheld Document on NSA Surveillance Program from Members*, Wash. Post, Aug. 16, 2013 28

President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) 14

President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Dec. 12, 2013) ..... passim

Primary Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 14-01 (FISC Jan. 3, 2014) 10

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* (Jan. 23, 2014) ..... passim

S. Rep. No. 95-604, pt.1 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904 6

Siobhan Gorman, *NSA Chief Opens Door to Narrower Data Collection*, Wall St. J., Feb. 27, 2014 52

Rules

Fed. R. Civ. P. 12 16

Fed. R. Crim. P. 17 51

FISC R. P. 17 6

FISC R. P. 62 6

INTRODUCTION

For more than a decade, the National Security Agency has been keeping a record of substantially all phone calls made or received on major U.S. telephone networks. Each time a resident of the United States makes a phone call, the NSA records whom she calls, when the call was placed, and how long the conversation lasted. The NSA keeps track of when she called the doctor, and which doctor she called; which family members she called, and which she did not; which pastor she called, and for how long she spoke to him. It keeps track of whether, how often, and precisely when she called the abortion clinic, the support group for alcoholics, the psychiatrist, the ex-girlfriend, the criminal-defense lawyer, the suicide hotline, and the child-services agency. The information collected under the program supplies the NSA with a rich profile of every citizen as well as a vast record of citizens' associations with one another. Indisputably, the NSA's surveillance is breathtaking in its scope and intrusiveness.

It is also unlawful. The statute the government relies on cannot be used to collect call records. Even if it could be used for this purpose, the phone-records program involves collection on a scale far beyond what the statute permits on its face, and far beyond what Congress intended. The government cannot demonstrate, as the statute requires it to, that there are reasonable grounds to believe that all

Americans' call records, over a twelve-year period (and counting), are "relevant" to an ongoing investigation.

The program would be anathema to the Constitution even if it were authorized by statute. It is unreasonable within the meaning of the Fourth Amendment. It also violates the First Amendment by unjustifiably intruding on Plaintiffs' associational privacy and by chilling communications that are central to Plaintiffs' work.

The district court erred in dismissing Plaintiffs' complaint and in denying their motion for a preliminary injunction. The ongoing surveillance of their associations is causing irreparable injury to Plaintiffs' privacy and associational rights. And both the balance of equities and the public interest favor injunctive relief. While the government once contended the program was the "only effective means" of tracking the associations of suspected terrorists, it has retreated from that claim in this litigation, and two government review groups—including a panel appointed by the President himself—have rejected it. Record evidence confirms that the government could achieve its stated goals without placing hundreds of millions of Americans under permanent surveillance.

The government does not have the authority to invade unnecessarily, and indefinitely, the privacy and associational rights of Plaintiffs and hundreds of millions of others. This Court should reverse the judgment below.

JURISDICTIONAL STATEMENT

Plaintiffs brought claims under the Constitution and the Administrative Procedure Act. The district court had subject-matter and personal jurisdiction pursuant to 28 U.S.C. § 1331 and 5 U.S.C. § 702. On December 27, 2013, the district court granted Defendants' motion to dismiss and denied Plaintiffs' motion for a preliminary judgment; the court entered final judgment the same day. SPA001–054; SPA055. On January 2, 2014, Plaintiffs timely filed their Notice of Appeal. JA393–394. This Court has jurisdiction under 28 U.S.C. § 1291.

ISSUES PRESENTED FOR REVIEW

1. Whether Plaintiffs' claim under Section 215 of the Patriot Act and the Administrative Procedure Act is impliedly precluded.

2. Whether the Stored Communications Act bars the government from using Section 215 to collect phone records.

3. Whether Section 215 authorizes the government's collection of phone records in bulk.

4. Whether the government's dragnet collection of phone records violates the Fourth Amendment.

5. Whether the government's dragnet collection of phone records violates the First Amendment.

6. Whether the district court erred in denying Plaintiffs' motion for a preliminary injunction.

STATEMENT OF THE CASE

Plaintiffs filed this lawsuit challenging the government's bulk collection of their phone records pursuant to Section 215 of the Patriot Act. Plaintiffs alleged that the collection violates Section 215 as well as the First and Fourth Amendments, and they sought injunctive relief. Plaintiffs moved for a preliminary injunction and Defendants moved to dismiss; the district court (Pauley, J.) denied Plaintiffs' motion and granted Defendants' motion. *See* SPA055; *ACLU v. Clapper*, No. 1:13-cv-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013). This appeal followed.

STATEMENT OF FACTS & PROCEDURAL HISTORY

The Foreign Intelligence Surveillance Act

Congress enacted the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, in 1978 to regulate government surveillance conducted for foreign-intelligence purposes. The Act was a response to *United States v. U.S. District Court* (*Keith*), 407 U.S. 297 (1972), in which the Supreme Court held that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. It was also a response to the Church Committee's finding that, over a period of decades, the executive branch had engaged in widespread warrantless surveillance of U.S. citizens—including journalists, federal judges, and Members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security." S. Rep. No. 95-604, pt.1, at 8 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3909 (quotation marks omitted).

In enacting FISA, Congress created the Foreign Intelligence Surveillance Court ("FISC") and empowered it to grant or deny government applications for surveillance orders in foreign-intelligence investigations. *See* 50 U.S.C. § 1803(a). The FISC meets in secret, generally hears argument only from the government, and does not ordinarily publish its decisions. *See, e.g.*, FISC R. P. 17(b), 62.

The provision at issue in this case was added to FISA in 1998. *See* 50 U.S.C. §§ 1861–1862 (2000). In its original form, it permitted the government to obtain an order compelling the production of certain records in foreign-intelligence or international-terrorism investigations from common carriers, public-accommodation facilities, storage facilities, and vehicle-rental facilities. *Id*. § 1862 (2000). The government was required to include in its application to the FISC "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power." *Id*.

The Patriot Act and several successor bills modified that provision in several respects. *See* USA PATRIOT Act of 2001, Pub. L. 107-56 ("Patriot Act"). In its current form, the provision—commonly called "Section 215," after the section of the Patriot Act that amended it—allows the government to obtain orders requiring the production of "any tangible things." 50 U.S.C. § 1861(a)(1). To obtain such orders, the government must supply the FISC with

> a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Id. § 1861(b)(2)(A). The provision deems certain kinds of tangible things "presumptively relevant." *See id.* § 1861(b)(2)(A)(i)–(iii).

Until recently, the public knew little about the government's use of Section

215. In 2011, Senators Ron Wyden and Mark Udall, both members of the Senate Select Committee on Intelligence, stated publicly that the government had adopted a "secret interpretation" of Section 215 and predicted that Americans would be "stunned" when they learned of it. 157 Cong. Rec. S3386 (daily ed. May 26, 2011) (statement of Sen. Ron Wyden); 157 Cong. Rec. S3389 (daily ed. May 26, 2011) (statement of Sen. Mark Udall). Their efforts to make more information available to the public, however, were largely unsuccessful, as were parallel efforts by Plaintiffs and others under the Freedom of Information Act. Ordinary citizens who wanted to understand the government's use of the statute were entirely reliant on the government's own statements, and those statements were sometimes misleading or false. *See, e.g.*, Glen Kessler, *James Clapper's "Least Untruthful" Statement to the Senate*, Wash. Post, June 12, 2013, http://wapo.st/170VVSu.

The NSA's Phone-Records Program

The government began collecting Americans' call records in bulk in the weeks after the September 11, 2001 terrorist attacks. *See* Public Declaration of James R. Clapper, Director of National Intelligence ¶ 6, *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal. Dec. 20, 2013), ECF No. 168. Initially, it collected the records without judicial authority, but on May 24, 2006, it obtained approval from the FISC to collect those records under Section 215. Order, *In re Application of the*

FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 06-05 (FISC May 24, 2006), http://1.usa.gov/1f28pHg.

The NSA's phone-records program remained secret until June 5, 2013, when *The Guardian* disclosed a previously secret "Secondary Order" that had been issued by the FISC two months earlier. JA114–117. The order directed Verizon Business Network Services ("Verizon") to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to every domestic and international call placed on its network between April 25, 2013 and July 19, 2013. JA115. It also specified that the "telephony metadata" was to include, for each phone call, the originating and terminating telephone number as well as the call's time and duration. *See id.* The government later authenticated the Secondary Order and acknowledged that the order had been issued as part of a broader program involving the collection of phone records from multiple telecommunications providers. SPA010; *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 1 (Aug. 9, 2013), http://bit.ly/15ebL9k ("White Paper"). The government also disclosed a Primary Order setting out the circumstances in which it could analyze and disseminate the information housed in its phone-records database. JA126–142.[1]

[1] FISC documents indicate that the government has violated the limits in the

The FISC did not issue an opinion explaining the program's legal basis until several months after the program was publicly revealed in June 2013. Since that time, it has issued two opinions analyzing the lawfulness of the program. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-109, 2013 WL 5741573 (FISC Aug. 29, 2013); JA310–332 (*In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-158 (FISC Oct. 11, 2013)). The FISC reauthorized the program most recently on January 3. *See* Primary Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 14-01 (FISC Jan. 3, 2014), http://1.usa.gov/1q7lbNv.

This Litigation and the Decision Below

Plaintiffs American Civil Liberties Union and American Civil Liberties Union Foundation are current customers of Verizon, the recipient of the Secondary Order. Until early April 2013, Plaintiffs New York Civil Liberties Union and New York Civil Liberties Union Foundation were also customers of Verizon. JA091 (Dunn Decl. ¶ 7). It is undisputed that Plaintiffs' phone records have been collected

---

Primary Order on multiple occasions. *See, e.g.*, Order at 6–7, 11, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13 (Mar. 2, 2009), http://1.usa.gov/1dtljBC (noting that the government "frequently and systematically violated" limitations imposed by the FISC).

by the NSA under the Secondary Order and that the collection of Plaintiffs' records continues "on an ongoing daily basis." JA115.

Plaintiffs commenced this litigation on June 11, 2013, alleging that the government's collection of their phone records exceeds statutory authority and violates the First and Fourth Amendments. Plaintiffs moved for a preliminary injunction that would, during the pendency of this litigation, bar the government from collecting their phone records under the program, require it to quarantine their phone records that it had already collected, and prohibit it from querying metadata obtained through the program with any phone number or other identifier associated with them.

On December 27, 2013, the district court denied Plaintiffs' preliminary-injunction motion and granted the government's motion to dismiss. The court acknowledged that the Administrative Procedure Act ("APA") generally waives sovereign immunity for suits against the United States that seek relief other than money damages, but it held that Congress had impliedly precluded claims under Section 215. SPA018–025. Addressing the merits of Plaintiffs' statutory claims nonetheless, the court rejected Plaintiffs' argument that the Stored Communications Act ("SCA") prohibits the government from using Section 215 to collect phone records. SPA026–027. The court also held that Section 215 authorizes the government to collect phone records "in bulk." The court wrote that

"'[r]elevance' has a broad legal meaning." SPA033. Here, the court reasoned, "the collection of virtually all telephony metadata is 'necessary' to permit the NSA . . . to do . . . algorithmic data analysis." SPA032. It also held that Congress had ratified the government's interpretation of Section 215 when it reauthorized the provision in 2010 and 2011. SPA028–032.[2]

Turning to Plaintiffs' constitutional claims, the court held that "[b]ecause *Smith* [*v. Maryland*, 442 U.S. 735 (1979),] controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment." SPA044. It then suggested that the First Amendment provides no protection distinct from the Fourth Amendment, SPA045–046, but ultimately declined to resolve that question in this case, holding that *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), "compels the conclusion that the bulk metadata collection does not burden First Amendment rights substantially," SPA046–047.

Notably, the district court's decision in this case was issued eleven days after another district court arrived at precisely the opposite conclusion on the Fourth Amendment question. In *Klayman v. Obama*, the court preliminarily enjoined the program after rejecting the argument that the issue was controlled by *Smith*. 957 F. Supp. 2d 1, 32 (D.D.C. 2013) (Leon, J.) ("[T]he surveillance program now before

[2] The court rejected the government's argument that the "mere" collection of Plaintiffs' phone records did not inflict an injury sufficient to support standing. SPA018.

me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search."). The court wrote that it could not "imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen." *Klayman*, 957 F. Supp. 2d at 42.

Developments Since December 2013

As the district courts in *Clapper* and *Klayman* were considering the lawfulness of the government's call-tracking program, two independent review groups appointed by President Obama—the President's Review Group on Intelligence and Communications Technologies ("PRG") and the Privacy and Civil Liberties Oversight Board ("PCLOB")—were evaluating the program as well. In comprehensive reports published in December 2013 and January 2014, the two groups roundly condemned the program on both legal and policy grounds. The PRG's unanimous report recommended that the government cease collection and storage of Americans' telephony metadata. PRG, *Liberty and Security in a Changing World* 17 (Dec. 12, 2013), http://1.usa.gov/1cBct0k ("PRG Report"). Though the PRG took no ultimate position as to the program's lawfulness, it suggested that the government's collection and storage of American's telephony metadata in bulk conformed neither to Section 215 itself, *see id.* at 86–89, nor to

the Fourth Amendment, *see id.* at 82. The PCLOB, though divided 3–2 on some of its recommendations, was even more emphatic:

> The Section 215 bulk telephone records program is not sustainable from a legal or policy perspective. . . . [T]he program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value.

PCLOB, *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* 168 (Jan. 23, 2014) ("PCLOB Report"), http://bit.ly/1d01flI.

On January 17, 2014, President Barack Obama gave a national address about the government's ongoing review of its signals-intelligence programs. *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://1.usa.gov/1l2zOBS. The President acknowledged that the phone-records program "could be used to yield more information about our private lives, and open the door to more intrusive bulk collection programs in the future." *Id.* In his speech, the President also announced his intention to seek modifications of the FISC orders governing the program. *Id.*

On February 5, 2014, the FISC approved those modifications, which "generally preclude the government from querying the telephony metadata without first having obtained, by motion, a determination by [the FISC] that each selection term to be used satisfies [a reasonable articulable suspicion] standard," and which

"limit the results of each query to metadata associated with identifiers that are within two, rather than three, 'hops' of the approved seed used to conduct the query." Order Granting the Government's Motion to Amend the Court's Primary Order Dated January 3, 2014, at 4, No. BR 14-01 (FISC Feb. 5, 2014), http://1.usa.gov/1l34PSi. Neither modification affects the program in a way that implicates Plaintiffs' challenge in this case.

SUMMARY OF THE ARGUMENT

The district court erred in granting Defendants' motion to dismiss and denying Plaintiffs' motion for a preliminary injunction. First, the phone-records program finds no support in the statute that purportedly authorizes it. Section 215 does not permit the government to acquire phone records. A separate statute, enacted as part of the same bill that contained Section 215, forbids the government from obtaining phone records except pursuant to specified authorities that do not include Section 215. Even if Section 215 permitted the government to acquire phone records, construing the statute to permit "bulk" collection requires distorting some of the statute's terms and ignoring others altogether.

Second, the program violates the Fourth Amendment. Phone records reveal personal details and relationships that most people customarily and justifiably regard as private. The government's dragnet collection of this information invades a reasonable expectation of privacy and constitutes a search. This search violates

the Fourth Amendment because it is warrantless and because it is far more intrusive than can be justified by any legitimate governmental interest.

Third, the program violates the First Amendment. Government surveillance that substantially burdens First Amendment rights, as this program does, must survive "exacting scrutiny." A program on this scale, however—one that involves the indefinite and dragnet collection of sensitive information about hundreds of millions of Americans—simply cannot survive that scrutiny.

The district court held that the public interest counsels against the entry of preliminary relief, but the government has no legitimate interest in conducting unlawful surveillance. Further—as the record shows, and as two recent executive-branch reports have recently confirmed—the government's legitimate interest in tracking suspected terrorists' associations can be accomplished through far less-intrusive means.

STANDARD OF REVIEW

The Court reviews *de novo* a district court's dismissal of a complaint pursuant to Federal Rule of Civil Procedure 12(b)(1) or (b)(6), accepting as true all material factual allegations in the complaint and drawing all reasonable inferences in the plaintiff's favor. *See Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 65 (2d Cir. 2012). When reviewing a court's denial of a preliminary injunction, this Court reviews the district court's legal conclusions *de novo*, its

findings of fact for clear error, and its ultimate decision for abuse of discretion. *See Zervos v. Verizon N.Y., Inc.*, 252 F.3d 163, 169 (2d Cir. 2001).

ARGUMENT

I. The district court erred in holding that the phone-records program is authorized by statute.

The district court erred in holding that the phone-records program is authorized by statute. Section 215 does not authorize the program, and other statutory provisions prohibit it.

A. Section 215 does not authorize the government to collect phone records.

On its face, Section 215 provides the government with general authority to compel the disclosure of tangible things. However, the Stored Communications Act ("SCA") specifically addresses the circumstances in which the government can compel the disclosure of phone records in particular. The SCA provision states that a "provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity." 18 U.S.C. § 2702(a)(3). While the SCA provision lists exceptions to its otherwise-categorical prohibition, *see id.* §§ 2702(c), 2703, Section 215 is not among them. This omission is particularly notable because Congress enacted sections 2702(c) and 2703 in the same bill as Section 215.

The district court held that Section 215 constitutes an implicit exception to Section 2702 because Section 215 orders "are functionally equivalent to grand jury subpoenas." SPA027. But well-settled rules of statutory construction require that the list of exceptions in section 2702 and 2703 be treated as exhaustive. *See United States v. Smith*, 499 U.S. 160, 167 (1991) ("Where Congress explicitly enumerates certain exceptions . . . additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent." (quotation marks omitted)). Congress has enacted a comprehensive scheme to regulate the government's collection of electronic communications and records relating to those communications. That comprehensive scheme, which addresses the precise circumstances in which the government can collect the records at issue in this case, must be given precedence over provisions that are more general. *See In re Stoltz*, 315 F.3d 80, 93 (2d Cir. 2002) (holding that it is a "basic principle of statutory construction that a specific statute . . . controls over a general provision" (quoting *HCSC–Laundry v. United States*, 450 U.S. 1, 6 (1981))); *see also* PCLOB Report 92–93.

Indeed, the Justice Department has *itself* acknowledged that it would contravene the structure of the SCA to "infer additional exceptions" to the "background rule of privacy" set out in section 2702(a). *See* Office of Legal Counsel, Memorandum Opinion for the General Counsel [of the] FBI: Requests for Information Under the Electronic Communications Privacy Act 3 (Nov. 5, 2008),

http://1.usa.gov/1e5GbvC (concluding that the FBI could not use national security letters to compel the production of records beyond those specifically exempted from the general privacy rule). Moreover, it has acknowledged that principle with respect to Section 215 itself, concluding that the statute does not override the privacy protections of the Census Act, 13 U.S.C. §§ 8, 9, 214. Letter from Ronald Weich, Assistant Attorney General, to Hon. Nydia Velázquez, Chair, Congressional Hispanic Caucus, U.S. House of Representatives (Mar. 3, 2010), http://wapo.st/aEsETd.

The legislative history of the 2006 amendments to Section 215 confirms that Section 215 was not intended to override privacy restrictions set out in other statutes. According to a 2007 report issued by the Justice Department's Office of the Inspector General, lawyers in the Justice Department were at one point concerned that educational-records laws limited their ability to use Section 215 to compel the disclosure of those records. *See* Office of the Inspector General, A Review of the FBI's Use of Section 215 Orders for Business Records x, xvi (2007), http://1.usa.gov/1cajBGI. To address this perceived defect in the statute, Congress added language in 2006 indicating that certain categories of records (including educational records) were subject to Section 215, despite applicable confidentiality provisions elsewhere. *See id.* at xvi; 50 U.S.C. § 1861(a)(3) (listing categories of records). That addition would have been unnecessary, of course, if

Section 215 overrode more specific privacy statutes, as the government now says it does.[3]

The district court reasoned that foreclosing the government from obtaining call records under Section 215, a provision that requires prior judicial review, would be "absurd" because the government can obtain call records with national security letters, which are issued without prior judicial review. SPA027. There are many reasons, however, why Congress might have wanted the government's collection of call records to be conducted under the administrative-subpoena provisions, particularly 18 U.S.C. § 2709, rather than under Section 215. Congress may have believed that the government's access to call-record information should be strictly limited to the categories of information set out in section 2709(b), which are more limited than the types of information the government now obtains under Section 215. It may have believed that the government's required disclosures to Congress about its collection of call records in foreign-intelligence investigations under section 2709(e) should be comprehensive. *See* PCLOB Report 94.

[3] Additionally, Section 215 lacks the "notwithstanding any other provision" language that appears elsewhere in FISA. *See, e.g.*, 50 U.S.C. § 1842(a)(1) (pen registers and trap-and-trace devices); *id*. § 1822(a)(1) (physical searches); *id*. § 1881a(a) (targeting of foreign persons outside the United States). The omission of that phrase makes even clearer that Section 215's general authority does not override statutory provisions that address certain classes of records more specifically.

But an inquiry into Congress's intent is unnecessary here because the language of the SCA is clear. *See United States v. Epstein*, 620 F.3d 76, 80 (2d Cir. 2010); *see also* PCLOB Report 95. The courts have declined to apply statutes as written only where doing so would produce a result "demonstrably at odds with the intentions of its drafters." *Demarest v. Manspeaker*, 498 U.S. 184, 190 (1991) (quoting *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 571 (1982)). This is not such a case. The government has pointed to no evidence whatsoever that Congress intended Section 215 to be used to collect call records—let alone to collect call records in bulk.[4]

B. Even if Section 215 authorizes the government to collect phone records, it does not authorize it to collect phone records on this scale.

Even if Section 215 authorizes the government to collect call records, the district erred in concluding that the statute authorizes the government to collect such records in "bulk." SPA032–036.

Section 215 grants broad authority, but it limits that authority in a number of ways. The government may obtain a Section 215 order only in connection with "an authorized investigation." 50 U.S.C. § 1861(b)(2)(A). The investigation must be a factually predicated one, not simply a "threat assessment." *Id*. The government may compel the production of tangible things only if there are reasonable grounds

[4] Indeed, the district court's reasoning renders FISA's pen register provision, 50 U.S.C. § 1842, entirely superfluous. *See* PCLOB Report 86.

to believe that those tangible things "are relevant" to its investigation, *id*., and only if they could be obtained with a grand jury subpoena or similar mechanism. *Id*. § 1861(c)(2)(D).

Here, however, the government has placed hundreds of millions of Americans under surveillance *not* because their phone records are believed to be "relevant," in any ordinary sense of the word, to any specific "authorized investigation," but on the theory that some small fraction of the records may become useful to a factually predicated investigation in the future. *See generally* JA126–142 (Primary Order); PCLOB Report 57–60. Moreover, the scale of the collection far exceeds what would be permissible with a grand jury subpoena or similar mechanism. Indeed, the government itself has conceded as much. Defendants' Mem. of Law in Supp. of Mot. to Dismiss 24, *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Aug. 26, 2013), ECF No. 33 (acknowledging that the case law relating to subpoenas "does not involve data acquisition on the scale of the telephony metadata collection").

Pointing to cases in which courts have upheld subpoenas that sought entire databases of records, the district court concluded that the records collected here are relevant as "a category." SPA036. But while the courts have sometimes upheld subpoenas for categories of information, those subpoenas were closely tied to, and limited by, the facts of specific investigations. They sought records of specific

individuals or corporations, or they sought records dealing with a specific subject matter, or they sought records created during a specific and limited time period. Courts have routinely quashed subpoenas that lacked a sufficient nexus to the investigation they were meant to advance. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951); *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (Friendly, J.) (narrowing grand jury subpoena because it improperly demanded the contents of multiple filing cabinets "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period"); *see also, e.g.*, *In re Six Grand Jury Witnesses*, 979 F.2d 939, 943 (2d Cir. 1992); *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 12–13 (S.D.N.Y. 1994).

The district court also concluded that the phone records are relevant because they are necessary to the application of certain analytic techniques. SPA032. "[W]ithout all the data points," the court reasoned, "the Government cannot be certain it connected the pertinent ones." *Id*. But the government did not contend in the court below that collecting the entire nation's phone records was necessary in this sense; it contended only that collecting those records was "one means" to track terrorists' communications. JA256 (Holley Decl. ¶ 30). Moreover, and as discussed at length below, *see infra* Part III.B.2, the government can track terrorists' communications *without* collecting everyone's phone records.

In any event, the courts have never construed the "relevance" requirement to allow the government to obtain whatever information it has the capacity to analyze. As the PCLOB noted, the implication of this reasoning would be that "if the government develops an effective means of searching through *everything* in order to find *something*, then *everything* becomes relevant to its investigations." PCLOB Report 62. The concept of "relevance" would be limited "only by the government's technological capacity to ingest information and sift through it efficiently." *Id*.

The district court reasoned that the government should be entitled to broader latitude here because Section 215 involves the counterterrorism context. SPA036. Many grand jury investigations, however, relate to terrorism or espionage, and yet no grand jury subpoena has ever reached as far as the NSA's phone-tracking program does. And other national security statutes use the same language used in Section 215—"relevant to an authorized investigation"—and yet none of these statutes has been interpreted in the way the district court interpreted Section 215 here.[5] If all Americans' call records are relevant to terrorism investigations, as the district court held they are, one would expect the government to have sought them before under one of these statutes or with a grand jury subpoena.

[5] *See, e.g.*, 18 U.S.C. § 2709(b)(1) (authorizing FBI to compel production of toll-billing and other records "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities"); 20 U.S.C. § 1232g(j)(1)(A) (authorizing Attorney General to compel production of educational records "relevant to an authorized investigation" related to terrorism).

Indeed, if all call records are relevant, many other sets of records are surely relevant as well. The government contends that bulk telephony metadata has "distinctive characteristics not common to most other types of records," Defs.' Mem. of Law in Opp. to Pls.' Mot. for a Preliminary Injunction 21, *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Oct. 1, 2013), ECF No. 66, but many records share the supposedly distinctive characteristics of call records, *see* JA307 (Suppl. Felten Decl. ¶¶ 11–12) (explaining that email metadata, internet-usage history, internet-chat records, financial records, credit-card records, "and even portions of medical records" are structured and interconnected, as call records are). The government's argument simply has no limit.

If Congress had intended to invest the government with the sweeping authority claimed here, it surely would have said so more directly. *See Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001) (Congress "does not, one might say, hide elephants in mouseholes."). Congress would not have used the same language used in run-of-the-mill administrative subpoena statutes. *See, e.g.*, 38 U.S.C. § 4326(a) (providing that the Secretary of Veterans Affairs shall have "the right to copy and receive . . . any documents of any person or employer that the Secretary considers relevant to the investigation"). It would not have expressly limited the scope of Section 215 orders to the kinds of information obtainable under grand jury subpoenas and similar instruments. And it would not have limited

the kinds of investigations that can serve as predicates for such orders. The government's theory of the statute is irreconcilable with the statute's plain text. Unsurprisingly, the legislator who authored Section 215 has emphasized that he never anticipated or intended that the government would use the statute as it using it now. Br. *Amicus Curiae* of Congressman F. James Sensenbrenner, Jr. in Supp. of Pls., *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. Sept. 4, 2013), ECF No. 46-1.[6]

C. Congress did not ratify the phone-records program when it reauthorized Section 215 in 2010 and 2011.

The district court held that Congress ratified the phone-records program when it reauthorized Section 215 in 2010 and 2011. SPA028–032. This, too, was error. Congress cannot ratify a statutory interpretation that contravenes the statute's plain meaning. *See Biddle v. Comm'r of Internal Revenue*, 302 U.S. 573, 582 (1938) ("Where the law is plain the subsequent re-enactment of a statute does not constitute adoption of its administrative construction."). Moreover, the ratification doctrine has relevance only where Congress was "well aware of" a judicial or administrative interpretation of its laws and where it "legislated on the basis of" that interpretation. *Atkins v. Parker*, 472 U.S. 115, 140 (1985). It has no

[6] Even if Section 215 does authorize the bulk collection of call records, it does not authorize their collection *by the NSA*. The government's program requires recipients to "produce to NSA" Americans' phone records—directly contradicting the statute's commands that "tangible things" be "made available to" or "received by" the FBI. *Compare* JA128 (Primary Order at 3), *with* 50 U.S.C. § 1861(b)(2)(B), (h); *see* PCLOB Report 87–91.

application here because Congress cannot be said to have been "well aware of" the phone-records program or of the FISC's interpretation of Section 215.

Although the district court held that the Congress had ratified "Section 215 as interpreted by . . . the FISC," SPA031, there was no FISC interpretation of Section 215 for Congress to ratify in 2010 and 2011. While the FISC authorized the phone-records program in 2006, it was not until 2013 that it issued an opinion explaining why it had done so. Congress cannot reasonably be presumed to have been fully aware of a judicial interpretation that did not yet exist.

Nor can Congress reasonably be said to have been fully aware of the *program* in 2010 and 2011. While the executive branch provided the congressional intelligence committees with briefing papers, the papers did not include any legal analysis. *See, e.g.*, JA151–155. Further, the papers were classified, and when the intelligence committees shared them with other members of Congress, they shared them under restrictive conditions. Legislators could examine the briefing papers only in secure locations in the offices of the intelligence committees, and for only a limited time. They were prohibited from making photocopies or taking notes. They were barred from discussing the program with each other, except in the secure facilities. They were barred from discussing it with their staffs. And, of course, they could not discuss the program with their constituents or debate it publicly. *See, e.g.*, Letter from Sen. Ron Wyden & Sen. Mark Udall to Eric Holder, Att'y

Gen. (Sept. 21, 2011), http://1.usa.gov/190sAls; Br. of *Amici Curiae* U.S. Representatives Amash et al. 3–4, *In re Orders Issued by This Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02 (FISC June 28, 2013), http://1.usa.gov/1cA7he5.

In other words, even the legislators who had access to the briefing papers had no "meaningful opportunity to gauge the legitimacy and implications of the legal interpretation in question." PCLOB Report 96; *see also United States v. Calamaro*, 354 U.S. 351, 359 (1957) (deeming reenactment to be "without significance" where it was "not accompanied by any congressional discussion which throws light on [the] intended scope" of the relevant interpretation).

Many Members of Congress did not have access to the briefing papers at all. Although the administration provided a classified briefing paper to the intelligence committees in 2011, the House Intelligence Committee did not share that briefing paper with Representatives who were not members of the Committee. *See* SPA031; Peter Wallsten, *House Panel Withheld Document on NSA Surveillance Program from Members*, Wash. Post, Aug. 16, 2013, http://wapo.st/1cTBZmh. The district court acknowledged that some legislators were not aware of the program before the reauthorization vote in 2011, but the court concluded that this was irrelevant because the executive had notified Congress in accordance with its statutory duty to do so. SPA031. The doctrine of legislative ratification, however,

is not a waiver doctrine, and accordingly the relevant question is not whether the executive complied with its statutory duty but whether Congress was, in fact, fully informed of the FISC's interpretation of Section 215. *Cf. Comm'r of Internal Revenue v. Glenshaw Glass Co.*, 348 U.S. 426, 431 (1955). Congress was not so informed.

II. The district court erred in holding that Plaintiffs' statutory claims are impliedly precluded.

Section 702 of the APA permits a "person suffering legal wrong because of agency action" to bring suit against the United States and its officers for "relief other than money damages." 5 U.S.C. § 702. Congress intended this waiver of sovereign immunity "to provide broadly for judicial review of [agency] actions, affecting as they do the lives and liberties of the American people." *Cohen v. United States*, 650 F.3d 717, 723 (D.C. Cir. 2011) (quoting *Natural Res. Def. Council v. Hodel*, 865 F.2d 288, 318 (D.C. Cir. 1988)).

Thus, the APA creates a "strong presumption" in favor of judicial review. *See, e.g.*, *Bowen v. Mich. Acad. of Family Practices*, 476 U.S. 667, 670 (1986); *see also Sackett v. EPA*, 132 S. Ct. 1367, 1373 (2012). The presumption may be overcome only with "clear and convincing evidence of a contrary legislative intent [to] restrict access to judicial review." *Bowen*, 476 U.S. at 671 (quotation marks omitted). Such evidence may be found in a statute's "express language, but also [in] the structure of the statutory scheme, its objectives, its legislative history, and

the nature of the administrative action involved." *Natural Res. Def. Council v. Johnson*, 461 F.3d 164, 171 (2d Cir. 2006). Ambiguity, if any, is resolved in favor of the APA's waiver: "[W]here substantial doubt about the congressional intent exists, the general presumption favoring judicial review of administrative action is controlling." *Id.* at 172.

The district court acknowledged the presumption in favor of judicial review, *see* SPA018–019, but, as explained below, it failed to give the presumption appropriate weight.

A. Plaintiffs' statutory claim is not precluded by 18 U.S.C. § 2712.

The district court held that Plaintiffs' statutory claim is precluded because 18 U.S.C. § 2712 "impliedly forbids" the injunctive relief that Plaintiffs seek. SPA019–021. However, it is plain from the structure of Section 2712, as well as from the relation of that provision to the larger statutory scheme, that Congress did not intend Section 2712 to displace the APA's waiver with respect to Section 215.

Section 2712 provides a cause of action for damages against the United States for willful violations of the SCA, the Wiretap Act, and three specific subsections of FISA: those relating to wiretapping, physical searches, and the installation of pen registers and trap-and-trace devices. *See* 18 U.S.C. § 2712(a). This damages remedy is "the exclusive remedy against the United States for any claims within the purview of [Section 2712]." *See* 18 U.S.C. § 2712(d). But

Section 2712 makes no mention of Section 215 or the subchapter in which it is found. Moreover, Section 2712(a) treats the SCA and Wiretap Act differently than it treats FISA, addressing the former two statutes categorically but addressing FISA's subchapters individually. *See* 18 U.S.C. § 2712(a). This underscores that Congress intended Section 2712's preclusive reach to extend not to *all* of FISA but only to the three specified subchapters of it.

The district court reasoned that Congress's failure to add a new damages clause to section 2712 when it amended Section 215 in 2006 indicates that Congress intended that there be no remedy for violations of Section 215 at all. SPA021. This does not follow. In 2006, Congress amended Section 215 to add a "use" provision similar to that contained in each of the three FISA subchapters referenced in section 2712(a). *See* 50 U.S.C. § 1861(h) (describing permissible uses of information obtained under Section 215); *id.* § 1806(a) (same for electronic surveillance); *id.* § 1825(a) (same for physical searches); *id.* § 1845(a) (same for pen registers). That Congress did not also amend section 2712 to add a *damages* remedy for "use" violations of Section 215 does not at all indicate that Congress intended to foreclose an *injunctive* remedy.

B. Plaintiffs' statutory claim is not precluded by Section 215.

The district court also held that Section 215 itself impliedly denies a right of judicial review to the *subjects* of Section 215 orders (such as Plaintiffs) by

expressly extending a right of judicial review to the *recipients* of such orders. SPA021–024. In so holding, the court misunderstood the legislative history and structure of Section 215 and misapplied relevant Supreme Court precedent.

There is no evidence that Congress's decision to address the review available to the recipients of Section 215 orders was intended to deny judicial review to the subjects of those orders. As originally enacted, Section 215 did not expressly provide for judicial review of orders issued under it. However, litigation filed by the recipient of a national security letter issued under 18 U.S.C. § 2709, *see Doe v. Ashcroft*, 334 F. Supp. 2d 471, 507 (S.D.N.Y. 2004), *aff'd in part*, *Doe v. Gonzale*s, 449 F.3d 415 (2d Cir. 2006), led Congress to address the review available to recipients of national security letters as well as to recipients of Section 215 orders. *See* 18 U.S.C. § 3511; 50 U.S.C. § 1861(f). The legislative history of those amendments makes clear that Congress's purpose was to clarify one species of judicial review, not to extinguish others. *See* H.R. Rep. 109-174, pt. 1, at 6, 77, 106 (repeatedly describing the addition of this subsection as an effort to "clarify" the statute). Indeed, in the debate preceding the amendments' enactment, the government concurred in the view that the amendments did not represent a significant change in the law.[7]

[7] See, e.g., Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary, 109th Cong. at 106 (2005) (testimony of Kenneth Wainstein, U.S. Att'y for the

The district court reasoned that extending a cause of action to the victims of surveillance would compromise the secrecy necessary to the government's surveillance efforts. SPA024. But Section 215 *itself* contemplates that the government's surveillance activities will be disclosed in some contexts. *See, e.g.*, 50 U.S.C. § 1861(f)(2)(C) (authorizing courts to vacate non-disclosure orders). The statute does not presume that the government's surveillance efforts will always and indefinitely remain secret.

More fundamentally, the district court's reasoning conflates the question of whether surveillance targets should be informed that the government is surveilling them with the question of whether targets *who already know that the government is surveilling them* should be allowed to challenge that surveillance. These are distinct questions, as this case illustrates. Allowing Plaintiffs to challenge the lawfulness of the phone-records program would not compromise government secrecy—the government has already acknowledged the surveillance that Plaintiffs are challenging. The district court asserted that the public should never have learned about the phone-records program, SPA025, but it surely cannot be the case that plaintiffs are foreclosed from challenging unlawful government conduct simply because the government wanted its unlawful conduct to be secret. And there would be something especially perverse about invoking such a rule in this

---

District of Columbia).

case, because senior government officials, including the Director of National Intelligence, have acknowledged that the phone-records program should not have been secret at all. *See, e.g.*, Eli Lake, *Spy Chief: We Should've Told You We Track Your Calls*, Daily Beast, Feb. 17, 2014, http://thebea.st/1kPoaZX.[8]

The district court relied heavily on *Block v. Community Nutrition Institute*, 467 U.S. 340 (1984), in which the Supreme Court considered whether the Agricultural Marketing Agreement Act ("AMAA") impliedly precluded a milk consumer from seeking judicial review of a "market order." *Id.* at 345–48. The AMAA authorized milk handlers to seek judicial review of market orders but was silent as to the remedies available to milk consumers. The Court held that in the context of the statutory scheme, Congress's silence as to milk consumers indicated that their claims were precluded. *Id.*

But neither *Block* nor any other case stands for the proposition that Congress's decision to extend the right of judicial review to one group precludes claims by all others. *See Sackett*, 132 S. Ct. at 1373 ("if the express provision of judicial review in one section of a long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it

[8] The district court also erred in stating that Plaintiffs' theory of the statute would "allow virtually any telephone subscriber to challenge a section 215 order." SPA024. If the phone-records program is susceptible to challenge from many telephone subscribers, this is a consequence not of Plaintiffs' theory of the statute but of the government's misuse of it.

would not be much of a presumption at all"); *see also Michigan v. U.S. Army Corps of Engineers*, 667 F.3d 765, 775–76 (7th Cir. 2011). Indeed, even as the *Block* Court held that Congress had intended to deny milk *consumers* the right to challenge market orders in court, it reaffirmed the right of milk *producers* to file such challenges—"even though the [AMAA] did not expressly provide them a right to judicial review." *Block*, 467 U.S. at 351 (citing *Stark v. Wickard*, 321 U.S. 288 (1944)). [9]

Moreover, several factors that were crucial to the Court's reasoning in *Block* are absent in this case.

First, the *Block* Court observed that extending a cause of action to milk consumers would have allowed an end run around the administrative-review requirements that the statute imposed on handlers. *Block*, 467 U.S. at 348. But Section 215 lacks any administrative-review requirement at all. *See* 50 U.S.C. § 1861.

Second, the *Block* Court observed that the statute at issue in that case, though it made reference to "general consumer interests," was enacted principally

[9] Notably, if Congress had intended to preclude the subjects of Section 215 orders from challenging those orders, it had language readily available to it. *See, e.g.*, 18 U.S.C. § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter."). The government would render provisions like this all but superfluous by imputing the same intent to Congress even in their absence.

to protect milk handlers and producers, not the consumers who were asking the Court to recognize a cause of action. *See Block*, 467 U.S. at 346–47 (describing the "principal purposes" of the statute as creating a "cooperative venture among the Secretary, handlers, and producers . . . to raise the price of agricultural products and to establish an orderly system for marketing them."). The provision at issue here, by contrast, is part of a statutory scheme specifically intended to protect the privacy of individuals like Plaintiffs, or at least to limit the circumstances in which the government may lawfully invade that privacy. *See, e.g.*, 124 Cong. Rec. 34, 845 (1978) (statement of Sen. Birch Bayh) ("This bill, for the first time in history, protects the rights of individuals from government activities in the foreign intelligence area.").

Third, the *Block* Court observed that Congress had extended a cause of action to another group—namely, milk handlers—whose interests were aligned with those of the consumers who sought to sue. *Block*, 467 U.S. at 352. Here, however, there is no alignment of interests between Plaintiffs and the telecommunications companies, the other group to which Congress has extended the right of judicial review. To the contrary, there are many reasons why their interests may diverge. Challenging Section 215 orders is time-consuming and costly. A telecommunications company that challenges a Section 215 order must sue the same government that regulates it. Moreover, a company that complies

with a Section 215 order is shielded from liability for having done so. 50 U.S.C. § 1861(e). Unsurprisingly, "no recipient of any Section 215 Order has challenged the legality of such an Order." *See In re Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted]*, 2013 WL 5741573, at *5.

That the interests of Plaintiffs are not aligned with those of telecommunications providers is a crucial point that the district court simply failed to consider, though Plaintiffs briefed it below and pressed it at oral argument. It was essential to the Supreme Court in *Block* that milk consumers' interests were aligned with those of the milk handlers who had been afforded the right to sue. And in applying *Block*, the appeals courts have given the alignment-of-interests question similar weight. *See, e.g.*, *Ark. Dairy Coop. Ass'n v. U.S. Dep't of Agric.*, 573 F.3d 815, 823 (D.C. Cir. 2009) (holding that milk producers had right of judicial review because they were "the only party with an interest in ensuring that the price paid to them" was fair); *Koretoff v. Vilsack*, 614 F.3d 532, 536–40 (D.C. Cir. 2010); *Council for Urological Interests v. Sebelius*, 668 F.3d 704, 710 (D.C. Cir. 2011). The Supreme Court and the D.C. Circuit have made clear that *Block* should not be read "too broadly," *Ark. Dairy*, 573 F.3d at 822–23, particularly

where the interests of the various parties diverge or the statute bears directly on the class to which the plaintiff belongs.[10]

III. The program violates the Fourth Amendment.

A. The government's bulk collection of phone records constitutes a search under the Fourth Amendment.

A Fourth Amendment search occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Under this test, the bulk collection of phone records constitutes a search. Americans do not expect that their government will make a note, every time they pick up the phone, of whom they call, precisely when they call them, and for precisely how long they speak. Nor should they have to. Generalized surveillance of this kind has historically been associated with authoritarian and totalitarian regimes, not with constitutional democracies. *See, e.g.*, Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1934 (2013) (Until recently, "the threat of constant surveillance has been relegated to the realms of science fiction and failed totalitarian states.").

[10] Plaintiffs believe that the phone-records program is inconsistent with the plain text of the Section 215, and that they are entitled to relief under the APA. If the Court concludes that the statute is ambiguous, however, the doctrine of constitutional avoidance weighs heavily against the sweeping construction of the statute that the government has adopted. *See, e.g.*, *Clark v. Martinez*, 543 U.S. 371, 381 (2005).

Neither the district court nor the government contested that Plaintiffs possess a subjective expectation of privacy in their phone records. *See, e.g.*, JA023–024 (Compl. ¶¶ 24–27); JA085–087 (Shapiro Decl. ¶¶ 3–5, 8); JA090–091 (Dunn Decl. ¶¶ 3, 5–6, 9); JA072, JA076–078, JA080–082 (German Decl. ¶¶ 2, 12–19, 23, 25–30). Rather, the district court dismissed Plaintiffs' Fourth Amendment claim based principally upon its conclusion that, under *Smith v. Maryland*, 442 U.S. 735 (1979), Plaintiffs' subjective expectation of privacy is not objectively reasonable. That conclusion was wrong. Nothing in *Smith* remotely suggests that the Constitution is blind to the kind of mass surveillance at issue here.

In *Smith*, the Baltimore police suspected that Michael Lee Smith was making threatening and obscene phone calls to a woman he had robbed days earlier. To confirm their suspicions, they asked Smith's telephone company to install a "pen register" on his line to record the numbers he dialed. After just a few days, the pen register confirmed that Smith was the culprit. The Supreme Court upheld the warrantless installation of the pen register in Smith's case, but the stakes were small. The pen register was very primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. *Id.* at 741. It was in place for only several days, and it was directed at a single criminal suspect. *Id.* at 737. Moreover, the information it

yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of other people. *Id*.

In other words, the question in *Smith* was only whether a specific individual—someone suspected of having committed a serious crime—had a reasonable expectation of privacy in the list of individuals he had called over the course of several days. Here, by contrast, the question is whether Plaintiffs—who are not criminal suspects—have a reasonable expectation of privacy in a catalogue of the phone numbers, date, time, and duration of every call they have placed or received over the last seven years and for the indefinite future. *Smith* did not address that question. *See Klayman*, 957 F. Supp. 2d at 31 (The question addressed in *Smith* was "a far cry from the issue in this case.").

Had *Smith* involved the kind of mass surveillance at issue here, the Supreme Court would undoubtedly have understood the case quite differently. Indeed, just four years after *Smith* was decided, the Court made explicit that dragnet surveillance presents a constitutional question altogether different than that raised by surveillance that is targeted. In *United States v. Knotts*, 460 U.S. 276 (1983), the Court considered the warrantless use of a beeper to track the car of a suspected manufacturer of illicit drugs. Citing *Smith*, the Supreme Court held that the defendant lacked a reasonable expectation of privacy in his public movements and that the governments' warrantless tracking of him did not violate the Constitution.

Id. at 281–85. The defendant argued that upholding the surveillance could lead to "twenty-four hour surveillance of any citizen of this country," *id.* at 283 (quotation marks omitted), but the Court disagreed that *Smith* could be so easily extended. "If such dragnet type law enforcement practices . . . should eventually occur," the Court wrote, "there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

The D.C. Circuit addressed the question left open by *Knotts* in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012), holding that the government's long-term tracking of an individual's movements amounted to a search for Fourth Amendment purposes. The Court rejected the government's argument that *Knotts* had already decided the issue. *Knotts*, the court explained, did not hold that an individual "has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it." 615 F.3d at 557.

The Supreme Court unanimously affirmed *Maynard* in *Jones*. All nine Justices in *Jones* agreed with the D.C. Circuit's conclusion that dragnet surveillance raises unique and novel questions, not controlled by prior precedent. *See Jones*, 132 S. Ct. at 954 ("It may be that achieving [long-term location tracking] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to

answer that question."); *id.* at 964 (Alito, J., concurring); *id.* at 955–56 (Sotomayor, J., concurring). Although the plurality opinion left that question for another day, five of the Justices, in two concurring opinions, made clear that they would resolve that question as had the D.C. Circuit. *See id.* at 964 (Alito, J., concurring) (concluding "that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment"); *id.* at 955 (Sotomayor, J., concurring) (concurring with Justice Alito's conclusion that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'").

Just as *Knotts* did not decide the issue presented in *Maynard* and *Jones*, *Smith* does not decide the issue presented here. Rather, the issue presented here must be resolved through the familiar inquiry described in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)—that is, by asking whether individuals have a reasonable expectation of privacy in the information the government seeks. *Smith* may be *relevant* to that inquiry, but so too is the observation, articulated by five of the Justices in *Jones*, that "longer term [electronic] monitoring"—even of information exposed to a third party—can implicate the Fourth Amendment. *See id.* at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring). As Justice Sotomayor recognized, long-term location tracking "enables the Government to ascertain, more or less at will, [every

person's] political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring).

What the *Jones* concurrences observed of location tracking is equally true of the bulk collection of Americans' call records. *See, e.g.*, JA018, JA026 (Compl. ¶¶ 1, 35). As the declaration of Professor Edward Felten explains, a comprehensive record of Americans' telephonic associations can reveal a wealth of detail about familial, political, professional, religious, and intimate relationships—the same kind of information that could traditionally be obtained only by examining the contents of communications. *See, e.g.*, JA049–058 (Felten Decl. ¶¶ 38–64); PCLOB Report 156–58. By aggregating metadata across time, the government can learn "when we are awake and asleep; our religion . . . ; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations." JA052 (Felten Decl. ¶ 46). It can learn about "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." JA056 (Felten Decl. ¶ 58). *See generally* PCLOB Report 12, 156–57; PRG Report 110–14, 116–17.

The district court reasoned that the government's collection of Plaintiffs' call records does not implicate the Fourth Amendment unless and until the

government analyzes the records, SPA040, but this is incorrect. The Fourth Amendment search takes place when the government collects Plaintiffs' telephony metadata in the first place. *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). Indeed, if this were not so, the Fourth Amendment would be indifferent to the government's warrantless recording of every phone call, or its warrantless copying of every email; the Constitution's protection would be triggered, if at all, only when the government listened to the calls or read the emails. This is not the law; nor should it be. The Fourth Amendment reflects the Framers' judgment that a neutral magistrate should be interposed between the government and the citizenry. Holding that the Fourth Amendment allows the government to search first and find suspicion later turns that principle on its head.[11]

The district court also erred in suggesting that Plaintiffs lack a protected privacy interest in their phone records because that information has been shared with a third party, namely Verizon. SPA042. *Jones* and other recent cases confirm

[11] In any event, the government *does* analyze Plaintiffs' call records—it does so every time it searches its phone-records database. *See Klayman*, 957 F. Supp. 2d at 28 & n.38 ("When the NSA runs such a query, its system must necessarily analyze metadata for every phone number in the database by comparing the foreign target number against *all* of the stored call records . . . .").

that the third-party doctrine is not, and has never been, an on–off switch. The mere fact that a person has shared information with the public or a third party does not mean that the person lacks a constitutionally protected privacy interest in it. *See* 132 S. Ct. at 957 (Sotomayor, J., concurring); *id*. at 964 (Alito, J., concurring); *Florida v. Jardines*, 133 S. Ct. 1409 (2013) (odors detectable by a police dog that emanate outside of a home); *Kyllo v. United States*, 533 U.S. 27 (2001) (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); *United States v. Knoll*, 16 F.3d 1313, 1321 (2d Cir. 1994) (unprivileged papers left with lawyer). Whether Plaintiffs have a reasonable expectation of privacy in their call records turns not on any binary test but on the totality of the circumstances. Americans do not expect that the government will track every phone call they make every single day, and they should not have to.[12]

[12] The district court was also wrong to suggest that Plaintiffs' call records are not sensitive unless the phone numbers in them are converted to identities. SPA041. Phone numbers, like social-security numbers, are identifying information. The government itself treats them as such under the Freedom of Information Act. *See, e.g.*, *Moore v. Obama*, No. 09-5072, 2009 WL 2762827, at *1 (D.C. Cir. Aug. 24, 2009) (per curiam). In any event, it is trivial to correlate phone numbers with subscriber names. JA043 (Felten Decl. ¶ 19 & n.14); JA304 (Suppl. Felten Decl. ¶¶ 3–4); PCLOB Report 22.

B. The government's bulk collection of telephony metadata is unreasonable.

Because the district court held that *Smith* controlled, it did not address at any length the question of whether the program is reasonable. It is not.

1. The phone-records program involves warrantless searches, which are per se unreasonable.

The program involves warrantless searches. Such searches "are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967); *see United States v. Karo*, 468 U.S. 705, 717 (1984). In fact, the program involves the particular form of search that the authors of the Fourth Amendment found most offensive—a general search predicated on a general warrant. *See Berger v. New York*, 388 U.S. 41, 59 (1967).

Like a general warrant, the program involves searches not predicated upon "an oath or information supplying cause." Morgan Cloud, *Searching Through History; Searching For History*, 63 U. Chi. L. Rev. 1707, 1738 (1996). Like a general warrant, it involves surveillance that "survive[s] indefinitely." *Id.* And like a general warrant, it is "not restricted to searches of specific places or to seizures of specific goods." *Id.*; *see also Berger*, 388 U.S. at 59 (striking down electronic-surveillance statute that, like "general warrants," left "too much to the discretion of

the officer executing the order" and gave the government "a roving commission to seize any and all conversations" (quotation marks omitted)).

In the district court, the government argued that the warrant requirement does not apply in this case because the phone-records program serves "special government needs." But the "special needs" doctrine applies "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see Ferguson*, 532 U.S. at 81–86; *City of Indianapolis v. Edmond*, 531 U.S. 32, 41–47 (2000).

Application of the warrant and individualized-suspicion requirements would not compromise the government's asserted interest in determining which individuals were in contact with phone numbers associated with suspected terrorists. *See infra* Part III.B.2. Even if one assumes, contrary to record evidence, JA305–306 (Suppl. Felten Decl. ¶¶ 6–8), that the phone-records program allows the government to learn terrorists' associations *more rapidly* than it would otherwise be able to, the Supreme Court has never dispensed with the Fourth Amendment's core constraints based on simple expedience. *See, e.g.*, *Carroll v. United States*, 267 U.S. 132, 153–54 (1925); *United States v. Barbera*, 514 F.2d 294, 301–02 (2d Cir. 1975). *See generally Keith*, 407 U.S. at 300, 320 (invalidating

warrantless wiretap authorized by the Attorney General "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government"). Moreover, in any true emergency the government could satisfy the exigent-circumstances exception to the warrant requirement. *See Missouri v. McNeely*, 133 S. Ct. 1552, 1570 (2013).

For these reasons, the special-needs doctrine does not apply in this case.

2. The government's bulk collection of telephony metadata is unreasonable.

Even if an exception to the warrant and probable-cause requirements applies, the phone-records program is unconstitutional because it is unreasonable. Courts have insisted that the government's intrusions on privacy be precise and discriminate. *See Berger*, 388 U.S. at 58. The phone-records program is anything but. To pursue its limited goal of tracking the associations of a discrete number of suspected terrorists, the government has employed the most indiscriminate means possible—collecting *everyone's* records. It has "scoop[ed] up the entire ocean to . . . catch a fish." Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, Wall St. J., July 8, 2013, http://on.wsj.com/14N9j6j (quoting Rep. Jim Sensenbrenner).

"[T]he ultimate touchstone of the Fourth Amendment" is "reasonableness," *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the "totality of circumstances" to "assess[], on the one hand, the

degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008). In the context of electronic surveillance, reasonableness demands that statutes be "precise and discriminate" and that the government's surveillance authority be "carefully circumscribed so as to prevent unauthorized invasions of privacy." *Berger*, 388 U.S. at 58 (quotation marks omitted).

The question here is whether the government's asserted interest in the phone-records program justifies the blanket invasion of Plaintiffs'—and every American's—right to privacy. It does not. The intrusion upon privacy is substantial: the government is tracking the phone calls of millions of innocent people. The records the government is collecting contain a wealth of information that can be every bit as revealing as the content of calls.

Yet the government is collecting all of these records without individualized suspicion, without temporal limit, and without limitation as to the individuals or phone calls swept up in the collection. It is collecting the records, in other words, under a program that lacks any of the traditional indicia of reasonableness. *See, e.g.*, *Berger*, 388 U.S. at 55–56, 59–60 (invalidating surveillance statute due to the breadth, lack of particularity, and indefinite duration of the surveillance it

authorized); *Chandler v. Miller*, 520 U.S. 305, 313 (1997) ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing."); *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (FISA's requirement of individualized suspicion that the government's target is an "agent of a foreign power" is part of what makes it "reasonable."); *United States v. Tortorello*, 480 F.2d 764, 773–74 (2d Cir. 1973) (Title III provides for "particularity in the application and order" and "clearly circumscribe[s] the discretion" of the government "as to when the surveillance should end."); *United States v. Cafero*, 473 F.2d 489, 496, 498 (3d Cir. 1973); *In re Sealed Case*, 310 F.3d 717, 739–40 (FISCR 2002).

The program also sweeps far more broadly than necessary to achieve the government's interests. The government's stated interest is in "identifying terrorist operatives and networks," JA260 (Shea Decl. ¶ 6), but there are many ways in which the government could achieve this goal without collecting the phone records of every U.S. resident. As the supplemental declaration of Professor Edward Felten explains, the government could issue targeted demands to the telecommunications companies to obtain, nearly instantaneously, the call records of suspected terrorists and individuals within "three hops" of them. JA305–306 (Suppl. Felten Decl. ¶¶ 6–8). The PRG and the PCLOB have similarly concluded that the government could achieve its goals without collecting phone records in bulk. PRG Report 118–19

("there are alternative ways for the government to achieve its legitimate goals, while significantly limiting the invasion of privacy and the risk of government abuse"); PCLOB Report 146 ("we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records").

In an effort to answer concerns about the phone-records program, the government stated that it queried the phone-records database fewer than 300 times in 2012. *See* White Paper 4. This statement, however, only confirms that the government could achieve its goals with targeted surveillance—that is, by serving the phone companies with demands for records relating to particular terrorism suspects. Multiple statutes permit the government to make such demands. *See, e.g.*, 50 U.S.C. § 1842 (pen registers in foreign-intelligence investigations); 18 U.S.C. § 2709 (national security letters); 18 U.S.C. §§ 3122, 3125 (pen registers in law-enforcement investigations); 18 U.S.C. § 2703(d) (orders for stored telephone records); Fed. R. Crim. P. 17(c).

Indeed, even the *government* appears to have concluded that it can achieve its goals without the dragnet collection of phone records. Although the government told the FISC in 2008 that bulk collection was the "only effective means" of tracking the associations of suspected terrorists, Order at 1–2, *In re Production of Tangible Things from [Redacted]*, No. BR 08-13 (Mar. 2, 2009), the government's

declarants in this case have conspicuously avoided that representation, stating instead that the program provides "one means" of tracking those associations, JA256 (Holley Decl. ¶ 30); *see* JA246 (*id.* ¶ 5) (program is "[o]ne method" of identifying terrorists); JA248 (*id.* ¶ 9) ("can contribute"); JA252 (*id.* ¶ 19) ("provides additional 'dots'"); JA260 (Shea Decl. ¶ 7) ("[o]ne method"). Just weeks ago, NSA Director Keith Alexander conceded publicly that the dragnet surveillance of Americans' call records is simply unnecessary. *See* Siobhan Gorman, *NSA Chief Opens Door to Narrower Data Collection*, Wall St. J., Feb. 27, 2014, http://on.wsj.com/1cA6SIr ("But Gen. Alexander instead signaled that the information the NSA needs about terrorist connections might be obtainable without first collecting what officials have termed 'the whole haystack' of U.S. phone data.").

The phone-records program is unreasonable because the far-reaching privacy intrusion it inflicts is, even on the government's own account, largely or entirely unnecessary to achieving the government's stated goals. The district court mistook Plaintiffs' complaint to be that the phone-records program is not the *least*-intrusive means of accomplishing the government's interests. SPA041. But Plaintiffs' argument is in fact quite different: the program is unreasonable because it is the *most*-intrusive means of accomplishing those interests. The availability of many targeted alternatives to its dragnet approach only underscores that fact.

IV. The program violates the First Amendment.

The district court also erred in dismissing Plaintiffs' claim that the phone-records program violates their First Amendment rights to private association and free speech. JA018–019, JA027 (Compl. ¶¶ 3, 37). Government surveillance that substantially burdens First Amendment rights, as the NSA's phone-records program does, must survive "exacting scrutiny." *See, e.g.*, *Buckley v. Valeo*, 424 U.S. 1, 64 (1976); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102–03 (2d Cir. 1985) (grand jury subpoena); *Clark v. Library of Cong.*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation). It is constitutional only if it serves a compelling state interest and only if it is the "least restrictive means" of achieving that interest. *See, e.g.*, *Clark*, 750 F.2d at 95. The phone-records program does not satisfy this standard.

A. The program substantially burdens Plaintiffs' First Amendment rights.

The district court erred in holding that the phone-records program does not cause any cognizable injury to Plaintiffs' First Amendment rights.

The program substantially impairs Plaintiffs' First Amendment rights because it exposes their telephonic associations to government monitoring and scrutiny. JA018–019, JA026 (Compl. ¶¶ 3, 35). In the course of their work, Plaintiffs routinely communicate by phone with their members, donors, current and potential clients, whistleblowers, legislators and their staffs, other advocacy

organizations, and members of the public. These communications are often sensitive or confidential; in many circumstances, this is true of the mere *fact* of the communication. *See* JA023–024 (Compl. ¶¶ 25–27); JA076–077 (German Decl. ¶¶ 12–13, 23–24); JA085–086 (Shapiro Decl. ¶ 4); JA091 (Dunn Decl. ¶¶ 5–6). The phone-records program impairs Plaintiffs' right of associational privacy by placing a record of all of these sensitive communications in the hands of the government.

The program also substantially impairs Plaintiffs' First Amendment rights by discouraging whistleblowers and others who would otherwise communicate with Plaintiffs from communicating with them. *See* JA023–024, JA026 (Compl. ¶¶ 25–27, 35); JA081–083 (German Decl. ¶¶ 28–32). The government's ongoing collection of Plaintiffs' call records has a chilling effect on associational activity that is integral to Plaintiffs' work.

The district court did not closely consider either of Plaintiffs' claims of injury, instead suggesting that its Fourth Amendment analysis made any First Amendment analysis unnecessary. SPA046. But the First Amendment provides protection distinct from the Fourth. *See, e.g.*, *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 269 (2d Cir. 1981) (narrowing subpoena as overbroad on First Amendment grounds); *Ealy v. Littlejohn*, 569 F.2d 219, 227 (5th Cir. 1978) ("the First Amendment can serve as a

limitation on the power of the grand jury"). Thus in *Tabbaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2007), which involved the government's search of U.S. citizens returning from a religious conference in Toronto, this Court conducted a First Amendment analysis even after concluding that the search had not violated the Fourth Amendment. The Court wrote:

> Our conclusion that the searches constituted a significant or substantial burden on plaintiffs' First Amendment associational rights is unaltered by our holding that the searches were routine under the Fourth Amendment. . . . [D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.

509 F.3d at 102 n.4.

To be sure, safeguards required by the Fourth Amendment may in some contexts satisfy the First Amendment as well—for example, a criminal search warrant may satisfy both the First and Fourth Amendments if it is carefully drawn and supported by probable cause. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 565 (1978); *United States v. Ramsey*, 431 U.S. 606, 623–24 (1977). But as the government's demands for information become more diffuse, implicating more and more protected information on a lower showing of need, the First Amendment calculus shifts too. *See Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963); *Local 1814*, 667 F.2d at 269; *FEC v. LaRouche Campaign*, 817

F.2d 233, 234–35 (2d Cir. 1987); *Paton v. La Prade*, 469 F. Supp. 773 (D.N.J. 1978).

The district court also erred in suggesting that any burden on Plaintiffs' First Amendment rights was not "substantial." SPA046. In fact, the scope of the NSA's phone-records program far exceeds that of the government surveillance that led to the Supreme Court's seminal associational-privacy cases, *NAACP v. Alabama*, *Bates*, 361 U.S. 516, and *Gibson*, 372 U.S. 539. While those cases involved demands for specific organizations' membership rolls, the metadata that the NSA is now gathering yields a much richer web of private associational information. It supplies a comprehensive map of the associational ties embedded in Plaintiffs' everyday work of public education, legal counseling and representation, and legislative advocacy. Although the government collects Plaintiffs' phone records from third parties, the program imposes the same burden on Plaintiffs' right to associational privacy as would a law requiring Plaintiffs themselves to report to the NSA at the end of each day whom they had called, when they had called them, and for how long they had spoken.

The chilling effect on Plaintiffs' contacts also effects a substantial impairment of Plaintiffs' First Amendment rights. The Supreme Court's decision in *Shelton v. Tucker*, 364 U.S. 479 (1960), is instructive. In that case, the Court found that First Amendment rights were substantially burdened by an Arkansas

law requiring teachers to "disclose every single organization with which [they had] been associated over a five-year period." *Id.* at 487–88 . In *Shelton*, this Court later observed, the Supreme Court "adopted a commonsense approach and recognized that a chilling effect was inevitable if teachers who served at the absolute will of school boards had to disclose to the government all organizations to which they belonged." *Local 1814, Int'l Longshoremen's Ass'n, AFL–CIO v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 272 (2d Cir. 1981). The chilling effect is equally inevitable here.

Finally, the district court erred in concluding that Plaintiffs' First Amendment argument was foreclosed by the Supreme Court's decision in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). The question in *Amnesty* was not whether Plaintiffs' rights had been impaired but whether Plaintiffs had standing to raise their claims at all when they had not established that their communications were being monitored. *Clapper*, 133 S. Ct. at 1148. Here, there is no dispute that Plaintiffs' call records are being collected, SPA017, and the district court itself concluded that Plaintiffs have standing, SPA017–018. To the extent the court relied on *Amnesty* for the proposition that Plaintiffs cannot make out a First Amendment claim without establishing that the government has "review[ed]" their records, the court misunderstood not only *Amnesty* but Plaintiffs' asserted injuries as well. The impairment of Plaintiffs' rights stems not from the government's

review of their records but from its collection of them in the first instance. It is the collection of those records that infringes Plaintiffs' associational privacy and that discourages whistleblowers and others from communicating with them.[13]

B. The phone-records program fails "exacting scrutiny" because it is unduly broad.

Because it held that any burden on First Amendment rights was insubstantial, the district court did not assess whether the program satisfies "exacting scrutiny." It does not. As discussed above, the program is the very definition of indiscriminate—the government is collecting *all* phone records because some tiny fraction of them may become useful to an investigation at some point in the future. *See* JA276 (Holly Decl. ¶¶ 58–59); *see also* PCLOB Report 58.

The courts have rejected investigative efforts that were far more discriminate than the one at issue here. In *Local 1814*, this Court narrowed a subpoena for payroll records after concluding that the subpoena would otherwise have an "inevitable chilling effect" on constitutionally protected activity. 667 F.2d at 273–74. The modification, the Court held, would "appropriately limit the impairment of . . . First Amendment rights without compromising the [government's] legitimate investigative needs." *Id*. at 274.

The Supreme Court's analysis in *Shelton* is likewise instructive. The Court

[13] In any event, the government *has* searched Plaintiffs' call records. *See supra* n.11.

characterized the law at issue in that case as "completely unlimited" because it required teachers to "list, without number, every conceivable kind of associational tie—social, professional, political, avocational, or religious." *Shelton*, 364 U.S. at 487–88. An inquiry into those associations could not be justified, the Court held, particularly when so many of them "could have no possible bearing" on the interests the government was seeking to protect. *Id.*; *see also Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972) (affirming refusal to answer grand jury questions on First Amendment grounds), *overruled in part on other grounds*, *In re Grand Jury Proceedings*, 863 F.2d 667, 669–70 (9th Cir. 1988); *In re Grand Jury Subpoena*, 701 F.2d 115, 119 (10th Cir. 1983) (remanding for evidentiary hearing to determine whether subpoena would chill associational rights and, if so, whether breadth of subpoena could be limited); *United States v. Citizens Bank*, 612 F.2d 1091, 1094–95 (8th Cir. 1980). Indeed, in this case the First Amendment analysis is more straightforward than it was in *Shelton* because it is plain that the government could achieve its legitimate goals with less intrusive means. *See supra* Part III.B.2.

The phone-records program needlessly encroaches on associational activity protected by the Constitution. It cannot survive the exacting scrutiny that the First Amendment requires.

V. The district court erred in denying Plaintiffs' motion for a preliminary injunction.

For the reasons stated above, Plaintiffs are likely to succeed on the merits of their claims. They are also likely to suffer irreparable injury if preliminary relief is not granted. *Citigroup Global Mkts., Inc. v. VCG Special Opportunities Master Fund Ltd.*, 598 F.3d 30, 35 (2d Cir. 2010). Indeed, this Court has generally *presumed* irreparable harm where there is an alleged deprivation of constitutional rights. *See, e.g.*, *Statharos v. N.Y. City Taxi & Limousine Comm'n*, 198 F.3d 317, 322 (2d Cir. 1999) (finding "no separate showing of irreparable harm is necessary" in case involving alleged invasion of privacy "[b]ecause plaintiffs allege deprivation of a constitutional right"); *Mitchell v. Cuomo*, 748 F.2d 804, 806 (2d Cir. 1984); *see also Covino v. Patrissi*, 967 F.2d 73, 77 (2d Cir. 1992) (applying presumption of irreparable harm in case alleging Fourth Amendment violations).

Here, Plaintiffs would satisfy the irreparable-harm standard even if the presumption did not apply. The continuation of the surveillance at issue means the continuation of the government's intrusion into Plaintiffs' sensitive associations and communications. When the government takes this private information for its own purposes, the injury is immediate—it is complete as soon as the government interjects itself into the zone of privacy. *Cf. United States v. Head*, 416 F. Supp. 840, 843 (S.D.N.Y. 1976) (zone of privacy includes areas "in which an individual has a reasonable expectation that governmental forces will not intrude"). The chill

on whistleblowers and others who would otherwise contact Plaintiffs is also immediate and irremediable. *See Mullins v. City of N.Y.*, 634 F. Supp. 2d 373, 392 (S.D.N.Y. 2009). And the government's queries of its call-records database compound Plaintiffs' injury. Each time the government queries the database for *any* identifier, it analyzes Plaintiffs' records in order to determine whether there are matches. *See supra* n.11. The resulting invasion of privacy is an injury that cannot be undone.

The district court also denied injunctive relief based on its assessment of the public interest. SPA047–051. The government has no legitimate interest, however, in conducting surveillance that violates both FISA and the Constitution. *Memphis Planned Parenthood, Inc. v. Sundquist*, 175 F.3d 456, 495 (6th Cir. 1999) ("[T]he public is certainly interested in preventing the enforcement of unconstitutional statutes and rules; therefore, no harm to the public will result from the issuance of the injunction here."); *see ACLU v. Ashcroft*, 322 F.3d 240, 247 (3d Cir. 2003). Moreover, the district court's assertion that "[t]he effectiveness of bulk telephony metadata collection cannot be seriously disputed," SPA048, is simply wrong. The President's own review group has called the program's effectiveness and necessity into question, PRG Report 118–19, as has the Privacy and Civil Liberties Oversight Board, PCLOB Report 146. The court stated that the phone-records program was crucial to certain terrorism investigations, but the record does not

support this claim, JA306 (Suppl. Felten Decl. ¶ 8), and the PCLOB, which reviewed "a wealth of classified materials" provided by the intelligence community, has expressly rejected it. PCLOB Report 145 (the program has not "yielded material counterterrorism results that could not have been achieved without" bulk collection); *see supra* Part III.B.2.

CONCLUSION

For the reasons stated above, this Court should reverse the judgment below and remand for entry of a preliminary injunction.

Dated: March 6, 2014

Respectfully submitted,

/s/ Jameel Jaffer

Jameel Jaffer
Alex Abdo
Patrick Toomey
Brett Max Kaufman
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

Christopher T. Dunn
Arthur N. Eisenberg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with Rule 32(a)(7)(B) because it contains 13,894 words, excluding the portions of the brief exempted by Rule 32(a)(7)(B)(iii), and that it complies with typeface and type style requirements of Rule 32(a)(5)-(6) because it is printed in a proportionally spaced 14-point font, Times New Roman.

/s/ Jameel Jaffer
Jameel Jaffer
Attorney for Plaintiffs–Appellants