UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

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

Plaintiffs,

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 ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

No. 13-cv-03994 (WHP)

ECF CASE

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Introduction

The National Security Agency ("NSA") has for seven years kept a record of every phone call made or received in the United States. The surveillance is ongoing. Each time a resident of the United States makes a phone call, the NSA records whom she called, 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 didn't; 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 fortune teller, the suicide hotline, the child-services agency, and the shelter for victims of domestic violence. The NSA keeps track of the same information for each of her contacts, and for each of *their* contacts. The data collected under the program supplies the NSA with a rich profile of every citizen as well as a comprehensive record of citizens' associations with one another.

Plaintiffs are civil-liberties organizations whose communications are particularly sensitive. Plaintiffs' employees routinely talk by phone with clients and potential clients about legal representation in suits against the government. Often, even the mere fact that Plaintiffs have communicated with these individuals is sensitive or confidential. Plaintiffs regularly receive calls from, among others, prospective whistleblowers seeking legal counsel and government employees who fear reprisal for their political views. The NSA has acknowledged that it is tracking all of these calls. This surveillance invades Plaintiffs' privacy, threatens to dissuade potential clients and others from contacting them, and compromises their ability to serve their clients' interests and their institutional missions.

Plaintiffs filed suit on June 11, 2013, contending that the NSA's ongoing tracking of their phone calls exceeds statutory authority and violates the First and Fourth Amendments. They

seek, among other things, an injunction permanently enjoining the mass call-tracking program and requiring the government to purge from its possession all of Plaintiffs' call records already collected. Plaintiffs now move this Court for a preliminary injunction that, during the pendency of this suit, (i) bars the government from collecting their call records under the program, (ii) requires the government to quarantine all of their call records already collected under the program, and (iii) prohibits the government from querying metadata obtained through the program using any phone number or other identifier associated with them.

Plaintiffs will suffer irreparable injury if preliminary relief is not granted, and they are substantially likely to succeed on the merits of their claims. The mass call-tracking program is ostensibly based on Section 215 of the Patriot Act but the program disregards that provision's core requirements, including its "relevance" requirement. The program violates the Fourth Amendment because the surveillance carried out is warrantless and unreasonable, and it violates the First Amendment because it substantially and unjustifiably burdens Plaintiffs' associational rights when more narrow methods could be used to achieve the government's ends. Indeed, the mass call-tracking program is perhaps the largest surveillance operation ever carried out by a democratic government against its own citizens. Preliminary relief is appropriate and necessary. *Cf. Stanford v. Texas*, 379 U.S. 476, 483 (1965) (citing eighteenth-century decision overturning a "ridiculous warrant against the whole English nation").

Legal and Factual Background

I. The Foreign Intelligence Surveillance Act

In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to regulate government surveillance conducted for foreign-intelligence purposes. Congress adopted FISA after the Supreme Court held, in *United States v. U.S. District Court* (*Keith*), 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence

investigations of domestic security threats. FISA was a response to that decision and to years of in-depth congressional investigation that revealed that the executive branch had engaged in widespread warrantless surveillance of U.S. citizens—including journalists, activists, 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 rarely publishes its decisions. *See, e.g.*, FISC R. P. 17(b), 62, http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

The provision at issue in this case was originally added to FISA in 1998. *See* 50 U.S.C. §§ 1861–1862 (2000 ed.). In its original form, it permitted the government to compel 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 ed.). 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.[1] In its current form, the statute—commonly referred to as Section 215—allows the government to

[1] The "Patriot Act" is the name customarily used to refer to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56. *See also* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. 107-108 (2001); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177 (2006).

obtain an order requiring the production of "any tangible things" upon a "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."[2]

While the amendments to this provision expanded the government's investigative power, this expansion was not without limits. Language added by the Patriot Act prohibits the government from using the provision to obtain tangible things that could not be obtained through analogous mechanisms. It states: "An order under this subsection . . . may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things." *Id.* § 1861(c)(2)(D).

Until recently, the public knew little about the government's use of Section 215. In 2011, Senators Ron Wyden and Mark Udall, both of whom sit on 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," "angry," and "alarmed" when they learned of it.[3] Their efforts to make more information available to the public, however, were

[2] *See* 50 U.S.C. § 1861(b)(2)(A) (deeming tangible things "presumptively relevant to an authorized investigation" if they pertain to "a foreign power or an agent of a foreign power"; "the activities of a suspected agent of a foreign power who is the subject of such authorized investigation"; or "an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation").

[3] 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).

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 surveillance policies were entirely reliant on the government's own statements about them, 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 (discussing statement by the Director of National Intelligence indicating, falsely, that government was not collecting information about millions of Americans).

II. The Mass Call-Tracking Program

On June 5, 2013, *The Guardian* disclosed a previously secret FISC order, labeled a "Secondary Order," directing 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.[4] The Secondary Order specified that telephony metadata includes, for each phone call, the originating and terminating telephone number as well as the call's time and duration. Secondary Order at 2. On the day the Secondary Order expired, the Director of National Intelligence issued a statement indicating that the FISC had renewed it. Office of the Dir. of Nat'l Intelligence, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata* (July 19, 2013), http://1.usa.gov/12ThYlT.

[4] Toomey Decl. Ex. 2 (Secondary Order at 2, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISA Ct. Apr. 25, 2013)) ("Secondary Order"). In the days after *The Guardian* disclosed the Secondary Order, Defendant Clapper acknowledged its authenticity. *See* Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), http://1.usa.gov/13jwuFc.

The government has disclosed that the Secondary Order was issued as part of a broader program that has been in place for seven years and that involves the collection of information about virtually every phone call, domestic and international, made or received in the United States. *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"); Dep't of Justice, *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization* 3 (Feb. 2, 2011), http://1.usa.gov/1cdFJ1G. The Secondary Order to Verizon was issued pursuant to a "Primary Order" that the government has now released and that sets out procedures the NSA must follow to "query" telephony metadata collected under the Secondary Order.[5]

The Primary Order and the administration's White Paper explain how the government analyzes and disseminates information housed in the massive database assembled by the call-tracking program. Specifically, the documents indicate that the NSA is permitted to query this database when a "designated approving official" at the NSA determines that "there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with" a "foreign terrorist organization." Primary Order at 7.[6] The NSA is permitted to review not just telephony metadata pertaining to the NSA's specific target but also telephony metadata pertaining to individuals as many as three degrees removed from that target:

[5] Toomey Decl. Ex. 1 (Primary Order at 3, 6–11, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-80 (FISA Ct. Apr. 25, 2013)) ("Primary Order").

[6] The government has acknowledged that the NSA has violated the Primary Order's restrictions on multiple occasions. White Paper at 5 ("Since the telephony metadata collection program under Section 215 was initiated, there have been a number of significant compliance and implementation issues that were discovered as a result of DOJ and ODNI reviews and internal NSA oversight.").

> Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers.

White Paper at 3–4. Even assuming, conservatively, that each person communicates by telephone with forty different people, an analyst who accessed the records of everyone within three hops of an initial target would have accessed records concerning more than two million people. The government has disclosed that the NSA conducted queries on approximately 300 selectors in 2012 alone. White Paper at 4.

III. Collection of Plaintiffs' Call Records

Plaintiffs American Civil Liberties Union and American Civil Liberties Union Foundation (together, "ACLU") are current customers of Verizon, which provides their wired communications service, including their landlines and internet connection. Shapiro Decl. ¶ 6. Until early April, Plaintiffs New York Civil Liberties Union and New York Civil Liberties Union Foundation (together, "NYCLU") were also customers of Verizon. Dunn Decl. ¶ 7. As current and former Verizon customers, Plaintiffs have had their telephony metadata collected in bulk pursuant to the Secondary Order and its predecessors. The NSA stores information collected under the program for five years.[7] Its collection of Plaintiffs' telephony metadata continues "on an ongoing daily basis." Secondary Order at 2.

[7] *See* Dep't of Justice, *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization* 4 (Feb. 2, 2011), http://1.usa.gov/1cdFJ1G; Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, Wall St. J., June 16, 2013, http://on.wsj.com/13MnSsp.

ARGUMENT

To justify entry of preliminary relief, Plaintiffs must show, first, that they are more likely than not to succeed on the merits of their claims at trial or on summary judgment; and, second, that they are 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). For the following reasons, preliminary relief is warranted here. Indeed, preliminary relief is warranted here even if Plaintiffs' motion is characterized as one that seeks "mandatory" relief. *See Mastrovincenzo v. City of N.Y.*, 435 F.3d 78, 89 (2d Cir. 2006) (noting that applicant for mandatory preliminary injunction must show "substantial likelihood" of prevailing).[8]

I. Plaintiffs are likely to succeed on the merits.

A. The government's long-term recording and aggregation of Plaintiffs' telephony metadata is not authorized by statute.

Section 215 allows the government to compel the production of tangible things if there are "reasonable grounds to believe that [they] are relevant to an authorized investigation." 50 U.S.C. § 1861(b)(2)(A). The mass call-tracking program goes far beyond this authority. First, the notion that detailed information about every phone call made by a resident of the United States over a seven-year period could be "relevant to an authorized investigation" finds no support in

[8] At the pre-motion conference, the Court requested that Plaintiffs address the Court's authority to review an order issued by a coordinate court. Plaintiffs do not believe that this case is properly characterized as a challenge to an order of a coordinate court. Plaintiffs are not seeking review of the Secondary Order; they are challenging the ongoing conduct of executive agencies. In any event, district courts review the lawfulness of FISC orders in the context of criminal prosecutions. *See* 50 U.S.C. § 1806(f); *see e.g.*, *United States v. Abu Jihaad*, 630 F.3d 102 (2d Cir. 2010); *United States v. Rahman*, 861 F. Supp. 247 (S.D.N.Y. 1994). More generally, courts often examine the legality of search or arrest warrants issued or approved by coordinate courts. *See Groh v. Ramirez*, 540 U.S. 551 (2004) (*Bivens* action); *United States v. Clark*, 638 F.3d 89 (2d Cir. 2011) (motion to suppress); *al Kidd v. Gonzales*, No. 1:05-CV-093-EJL-MHW, 2012 WL 4470776 (D. Idaho Sept. 27, 2012) (*Malley* claim). Even if this case is framed as one requesting review of the Secondary Order, the Court has ample authority to do so.

precedent or common sense. The program assigns "relevance" either a strained and altogether novel meaning—one that no court has previously accepted—or no meaning at all. Second, the program impermissibly transforms a statutory provision that was meant to permit the collection of existing records into one that permits the ongoing collection of records not yet in existence. This contravenes the text of Section 215 and makes nonsense of the larger statutory scheme. Third, the program replaces judicial supervision over the acquisition of information with executive discretion over the later use of information. The mass call-tracking program is the product of statutory alchemy; there is simply no way to justify it without rewriting the statute altogether.[9]

The billions of call records acquired under the mass call-tracking program every day are not "relevant to an authorized investigation" in any conventional sense of that phrase. In ordinary usage, one thing is said to be relevant to another if there is a demonstrably close connection between them. *See Oxford American Dictionary* 1474 (3d ed. 2010) ("the state of being closely connected or appropriate to the matter in hand"); *Webster's Collegiate Dictionary* 1051 (11th ed. 2012) ("having significant and demonstrable bearing on the matter at hand"). And, as discussed below, courts have consistently applied that ordinary meaning to require that records demanded

[9] Many Members of Congress have noted as much. *See, e.g.*, Rep. Jim Sensenbrenner, *How Secrecy Erodes Democracy*, Politico, July 22, 2013, http://politi.co/1baupnm (op-ed by original sponsor of Patriot Act) ("This expansive characterization of relevance makes a mockery of the legal standard. According to the administration, everything is relevant provided something is relevant. Congress intended the standard to mean what it says: The records requested must be reasonably believed to be associated with international terrorism or spying. To argue otherwise renders the standard meaningless."); *Oversight of the Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. at 1h:19m:40s (July 17, 2013), http://1.usa.gov/131CkgJ ("HJC Hearing") (statement of Rep. Jerrold Nadler, Member, H. Comm. on the Judiciary) ("If we removed that word from the statute, [the government] wouldn't consider . . . that it would affect [its] ability to collect meta-data in any way whatsoever—which is to say [it's] disregarding the statute entirely.").

by the government—through, for example, grand-jury subpoenas—bear an actual connection to a particular investigation.

The core problem with the government's approach to "relevance" is that the government cannot possibly tie the bulk collection of Americans' call records to a specific investigation, as the statute requires. Indeed, the government has conceded that few of the records collected under the mass call-tracking program have any connection to any investigation. *See, e.g.*, Letter from Peter J. Kadzik, Principal Deputy Assistant Att'y Gen., Dep't of Justice, to Rep. F. James Sensenbrenner, Jr. 2 (July 16, 2013), http://1.usa.gov/12GN8kW (conceding that "most of the records in the dataset are not associated with terrorist activity"). Most of the records swept up by the program—in fact, almost all of them—are what would ordinarily be called "irrelevant."

Thus, the program guts the concept of relevance of its usual meaning—indeed, of *any* meaning. Section 215 requires the government to distinguish relevant records from irrelevant ones, but the program relies on collapsing the two categories. It renders the concept of irrelevance irrelevant. *See United States v. Menasche*, 348 U.S. 528, 538–39 (1955) (It is the Court's "duty 'to give effect, if possible, to every clause and word of a statute,' rather than to emasculate an entire section, as the Government's interpretation requires." (citation omitted) (quoting *Inhabitants of Montclair Twp. v. Ramsdell*, 107 U.S. 147, 152 (1883))).

The concept of relevance has "developed a particularized legal meaning in the context of the production of documents and other things in conjunction with official investigations and legal proceedings." White Paper at 9. In these other contexts, courts have generally given "relevance" a broad compass. *See, e.g., Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 587 (1993); *United States v. R. Enters., Inc.*, 498 U.S. 292 (1991). To say that courts have given relevance a broad compass, however, is not to say they have given it a boundless one. The

relevance standard allows courts to prevent abuses of the judicial process, to protect individuals and corporations from unwarranted harassment, and to serve society's interest in limiting the costs and delays of litigation. *See, e.g.*, *United States v. Powell*, 379 U.S. 48, 57–58 (1964); *Resolution Trust Corp. v. Dabney*, 73 F.3d 262, 269 (10th Cir. 1995); *United States v. Westinghouse Elec. Corp.*, 788 F.2d 164, 166–67 (3d Cir. 1986).

Accordingly, courts routinely quash subpoenas for records that do not have a direct relationship to the underlying investigation they are meant to serve. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating a subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts also reject or narrow subpoenas that, because they fail to identify the outer bounds of the categories of documents they seek, cover large volumes of *irrelevant* documents. *See In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (Friendly, J.) (narrowing a grand-jury subpoena on the grounds that 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"); *cf. Cheney v. U.S. Dist. Court*, 542 U.S. 367, 387–88 (2004) (approving of circuit court's reversal of "overbroad" discovery orders that were "anything but appropriate" because they "ask[ed] for everything under the sky"); *In re Six Grand Jury Witnesses*, 979 F.2d 939, 943 (2d Cir. 1992) ("All agree that the rules of discovery are to be applied broadly, but that according the discovery rules liberal treatment does not license opposing counsel to discover anything and everything.").

This Court has applied that same logic to quash a subpoena duces tecum that demanded the entirety of the content of "computer hard drives and floppy disks," finding it overbroad because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry." *In*

re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (Mukasey, J.). In *In re Grand Jury Subpoena*, as in this case, government counsel acknowledged that the subpoena requested the production of irrelevant documents. *Id.* at 13. Comparing the hard drives in the case before him to the filing cabinets in *In re Horowitz*, Judge Mukasey quashed the subpoena. The Court concluded that the government could, by using keyword searches, "isolate[]" the relevant documents without requiring the subject of the subpoena to turn over the irrelevant ones. *Id.* And notably, the Court rejected the government's contention that its "more sweeping demand than might normally be made" was justified by the breadth of its investigation, as even an "expanded investigation does not justify a subpoena which encompasses documents completely irrelevant to its scope." *Id.* (quotation marks omitted).[10]

The license to collect relevant records is not, as the government would have it, a license to collect everything. In its public defense of the mass call-tracking program, the government has suggested that all of the records collected under the program are relevant because some of them might become useful in the future. *See generally* HJC Hearing. Unless cabined in some way, however, this theory would justify the collection of virtually *any* record. It is always *possible*, after all, that information not known to be relevant now will become relevant later. Section 215,

[10] *See also Cessante v. City of Pontiac*, No. CIV. A. 07-CV-15250, 2009 WL 973339, at *7 (E.D. Mich. Apr. 9, 2009) ("While some of the information sought may be relevant or lead to relevant information, the request for 'anything and everything' is overly broad and not narrowly tailored to meet the relevancy requirements of Fed. R. Civ. P. 26(b)."); *Hale v. Henkel*, 201 U.S. 43, 76–77 (1906) (finding a "*subpoena duces tecum* . . . far too sweeping in its terms to be regarded as reasonable" where it did not "require the production of a single contract, or of contracts with a particular corporation, or a limited number of documents, but all understandings, contracts, or correspondence between" a company and six others, among other broadly stated requests spanning many years and locations); *Ealy v. Littlejohn*, 569 F.2d 219, 227 (5th Cir. 1978) (tying First Amendment limitations on grand-jury investigations to "relevancy to the crime under investigation," and concluding that "[w]hen the grand jury goes on a fishing expedition in forbidden waters, the courts are not powerless to act").

however, does not authorize the government to compel the production of records simply because they might one day become relevant. It authorizes the collection of records only if there are reasonable grounds to believe that they "*are*" relevant. 50 U.S.C. § 1861(b)(2)(A) (emphasis added); *see In re Fontaine*, 402 F. Supp. 1219, 1221 (E.D.N.Y. 1975) ("While the standard of relevancy is a liberal one, it is not so liberal as to allow a party 'to roam in shadow zones of relevancy and to explore matter which does not presently appear germane on the theory that it might conceivably become so.'" (quoting *In re Surety Ass'n of Am.*, 388 F.2d 412, 414 (2d Cir. 1967))).[11]

Section 215 was meant to supply the government in the foreign-intelligence context with the same kind of authority that it possessed already in the law-enforcement context. *See* Dep't of Justice, *USA PATRIOT Act: Myth vs. Reality*, http://1.usa.gov/14nej54 (last visited Aug. 22, 2013) ("Obtaining business records is a long-standing law enforcement tactic. . . . Section 215 authorized the FISA court to issue similar orders in national-security investigations." (emphasis omitted)); 50 U.S.C. § 1861(c)(2)(D).

By the government's own admission, however, no court has ever sanctioned a subpoena that sought production on the scale of the mass call-tracking program. *See, e.g.*, White Paper at 11 ("To be sure, the cases that have been decided in these contexts do not involve collection of data on the scale at issue in the telephony metadata collection program, and the purpose for which information was sought in these cases was not as expansive in scope as a nationwide intelligence collection effort designed to identify terrorist threats."). Nor, again, is there any serious argument that such a sweeping subpoena would be upheld.

[11] Notably, while a presumption of regularity attaches to all grand-jury subpoenas and thus places the burden to quash on the recipients, *see, e.g.*, *Powell*, 379 U.S. at 58; *In re Grand Jury Proceedings*, 486 F.2d 85, 92 (3d Cir. 1973), Section 215 applies a presumption of relevance to only three narrow categories of tangible things. 50 U.S.C. § 1861(b)(2)(A).

The program also exceeds statutory authority because it involves surveillance that is prospective rather than retrospective. On its face, Section 215 permits the government to collect already-existing records, not to engage in ongoing surveillance. *See* 50 U.S.C. § 1861(c)(1)–(2) (contemplating the "release" of "tangible things" that can be "fairly identified" after a "reasonable period of time within which the tangible things can be assembled and made available"). The government has acknowledged this. *See, e.g.*, HJC Hearing at 3h:00m:03s (statement of Robert Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence) ("It's important to remember that 215 authority allows you to acquire existing records and documents and it's limited to that."). Here, however, the government has subjected recipients of Section 215 orders to an ongoing production obligation—an obligation that is effectively indefinite.

Moreover, the government's use of Section 215 here amounts to an end run around other FISA provisions that specifically address—and limit—the circumstances in which the government can engage in prospective surveillance of telephony metadata. *See* 50 U.S.C. § 1842(a) (authorizing installation and use of "pen register" and "trap and trace" device); *id.* at § 1842(d) (stating that order granting approval to install or use "pen register" or "trap and trace" device must include, among other things, "the identity, if known, of the person who is the subject of the investigation"; "the identity, if known" of the person whose telephone is to be monitored; and "the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order"). The government is improperly relying on Section 215 to engage in conduct that a more specific provision—namely, 50 U.S.C. § 1842—disallows. *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))).[12]

Finally, the mass call-tracking exceeds statutory authority because it effectively reassigns to the executive a task that Congress assigned to the judiciary. Section 215 entrusts to the FISC, not the executive, the responsibility of determining whether the "tangible things" sought by the government are closely connected to an authorized investigation. Under the mass call-tracking program, however, that determination is shifted entirely to the executive. *See* White Paper at 3–4 (describing process by which executive officers determine whether and how already-collected metadata should be queried). Again, the government has acknowledged that the vast majority of the records collected under the program have no connection at all to terrorism. Its defense of the program is that executive officers make a nexus determination when they *access* the database. If that is how Congress had wanted the statute to operate, it could readily have said so. It is easy to understand why Congress did not. *See, e.g.*, Memorandum Opinion, *[Title Redacted]*, No. 11 BR [Dkt. No. Redacted], at 16 n.14 (FISA Ct. Oct. 3, 2011) (Bates, J.), http://bit.ly/13UH2dS (discussing a previous FISC ruling) ("Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been so frequently and systematically violated that it can fairly be said that this critical element of the overall

[12] Notably, concerns about an analogous end run have led some courts to prohibit the government from using the Stored Communications Act ("SCA") to engage in prospective surveillance of telephony metadata for law-enforcement purposes. *See In re Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info.*, No. 6:08-6038M-REW, 2009 WL 8231744, at *3, *8 (E.D. Ky. Apr. 17, 2009) (discussing language in the SCA "plainly indicat[ing]" that it applies only to "records/information that exist at the time of application"); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (discussing the availability of surveillance tools that are more appropriate authorities for forward-looking record collection because they are "inherently prospective in nature").

regime has never functioned effectively." (alteration and quotation marks omitted)). In substituting the executive's ex post nexus determination for the FISC's ex ante relevance determination, the program exceeds statutory authority.

For the foregoing reasons, the program cannot be reconciled with Section 215's plain language. *See BedRoc Ltd. v. United States*, 541 U.S. 176, 183 (2004) ("[O]ur inquiry begins with the statutory text, and ends there as well if the text is unambiguous.").[13]

B. The government's long-term recording and aggregation of Plaintiffs' telephony metadata violates the Fourth Amendment.

The mass call-tracking program is unlawful under the Fourth Amendment. Telephony metadata reveals personal details and relationships that most people customarily and justifiably regard as private. The government's long-term recording and aggregation of this information invades a reasonable expectation of privacy and constitutes a search. This search violates the Fourth Amendment because it is warrantless and unreasonable. Indeed, it lacks any of the usual indicia of reasonableness: it infringes Plaintiffs' privacy without probable cause or individualized suspicion of any kind; it is effectively indefinite, having been in place for seven years already; and it lacks any measure of particularity, instead logging information about every single phone call.

1. The government's long-term recording and aggregation of telephony metadata 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.

[13] For the reasons stated above, Plaintiffs believe that the mass call-tracking program is inconsistent with the plain text of the Section 215. Even if the court concludes that the provision's text is ambiguous, however, the doctrine of constitutional avoidance counsels rejection of the sweeping construction of the provision that the government appears to have adopted. *See, e.g.*, *Clark v. Martinez*, 543 U.S. 371, 381 (2005); *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Const. Trades Council*, 485 U.S. 568, 575 (1988).

27, 33 (2001). Under this test, the long-term recording and aggregation of telephony metadata 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.*, *United States v. Gordon*, 236 F.2d 916, 919 (2d Cir. 1956); 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."); George Orwell, *Freedom and Happiness*, Tribune, Jan. 4, 1946 (review of Yevgeny Zamyatin's *We*), http://bit.ly/GCmoHe; *The Lives of Others* (Sony Pictures Classics 2006).

As an initial matter, Plaintiffs have a subjective expectation of privacy in their telephony metadata.[14] As the declarations of Steven R. Shapiro, Christopher Dunn, and Michael German explain, Plaintiffs ACLU and NYCLU work on a wide range of civil-liberties and human-rights issues, including issues relating to national security, police accountability, reproductive rights, LGBT rights, and immigrants' rights. Shapiro Decl. ¶ 3; Dunn Decl. ¶ 3; German Decl. ¶ 2. In connection with this work, ACLU and NYCLU staff frequently place calls to, and receive calls from, individuals who have been wronged in some way by the government, have knowledge of government abuses, or fear government retaliation for some action they have taken in the past. German Decl. ¶¶ 12–19; Shapiro Decl. ¶¶ 4, 8; Dunn Decl. ¶¶ 5–6, 9. These communications are

[14] Most Americans apparently agree that their telephony metadata should be secure from long-term recording and aggregation by the government. *See, e.g.*, Frank Newport, *Americans Disapprove of Government Surveillance Programs*, Gallup Politics, June 12, 2013, http://bit.ly/11fWoZc; Pew Research, *Few See Adequate Limits on NSA Surveillance Program*, July 26, 2013, http://bit.ly/12pdN7D; *see also* Press Release, Office of Sen. Ron Wyden, *Wyden Statement on Alleged Large-Scale Collection of Phone Records*, June 6, 2013, http://1.usa.gov/11v2Deo ("Collecting this data about every single phone call that every American makes every day [is] a massive invasion of Americans' privacy.").

often sensitive or confidential; in many circumstances, this is true of the mere *fact* of the communication. For example, Plaintiffs routinely communicate with prospective whistleblowers who would forgo speaking with Plaintiffs if they believed that their communications were being logged by the government. *See, e.g.*, Shapiro Decl. ¶¶ 4, 8; German Decl. ¶¶ 23, 25–30.

Because its communications are often sensitive or confidential, the ACLU takes measures to protect its communications from surveillance by the government or other third parties. *See, e.g.*, Shapiro Decl. ¶ 5. In some circumstances ACLU staff use encryption software to protect the substance of their communications. *Id.* The ACLU is not aware of any technology that would allow it to shield its telephony metadata from surveillance of the kind at issue here, *see* Felten Decl. ¶¶ 30, 33–37, but Plaintiffs treat their telephony metadata as sensitive. Shapiro Decl. ¶ 5.[15]

Plaintiffs' expectation that their telephony metadata will not be subject to long-term recording and aggregation by the government is objectively reasonable. The kind of surveillance at issue here permits the government to assemble a richly detailed profile of every person living in the United States and to draw a comprehensive map of their associations with one another. As the declaration of Edward Felten explains, "analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications." Felten Decl. ¶ 39. For example, "certain telephone numbers are used for a

[15] The reasonableness of Plaintiffs' expectation of privacy is reinforced by the terms of service in their contracts with Verizon, which describe Verizon's obligation to protect the confidential information its subscribers necessarily share in the course of their communications. These agreements define Customer Proprietary Network Information ("CPNI") to include, among other things, "information relating to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications services Customer purchases from Verizon, *as well as related local and toll billing information, made available to Verizon solely by virtue of Customer's relationship with Verizon*." Shapiro Decl. ¶ 7 (emphasis added). Consistent with privacy protections written into federal law, 47 U.S.C. § 222(c)(1), Verizon agrees to "protect the confidentiality of Customer CPNI in accordance with applicable laws, rules and regulations." Shapiro Decl. ¶ 7.

single purpose," *id.* ¶ 40, and their use can reveal a person's religion, political associations, use of a phone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes. *Id.* ¶¶ 39–45. "The phone records indicating that someone called a sexual hotline or a tax fraud reporting hotline will . . . reveal information that virtually everyone would consider extremely private." *Id.* ¶ 42.

Aggregating metadata across time can yield "an even richer repository of personal and associational details." *Id.* ¶ 47. Even basic inspection of our calling patterns, without relying upon single-use numbers, can reveal: "when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations." *Id.* ¶ 46. It "can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant." *Id.* ¶ 58.

Finally, aggregating the telephony metadata of many people allows researchers to "observe even deeper patterns." *Id.* ¶ 59. Because individuals are often defined by the company they keep, pooling together one person's telephony metadata with the telephony metadata of each of her contacts and each of her contacts' contacts allows an analyst to "paint[] a picture that can be startlingly detailed." *Id.* ¶ 1. As Professor Felten writes, "The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people." *Id.* ¶ 64.

The long-term recording and aggregation of telephony metadata achieves essentially the same kind of privacy intrusion that led five Justices of the Supreme Court to conclude in *United States v. Jones*, 132 S. Ct. 945 (2012), that the long-term recording and aggregation of location information constituted a search. In *Jones*, the Supreme Court considered whether police had conducted a Fourth Amendment search when they attached a GPS-tracking device to a vehicle and monitored its movements over a period of twenty-eight days. The Court held that the installation of the GPS device and the use of it to monitor the vehicle's movements constituted a search because it involved a trespass "conjoined with . . . an attempt to find something or to obtain information." *Id*. at 951 n.5. In two concurring opinions, five Justices concluded that the surveillance constituted a search because it "impinge[d] on expectations of privacy." *Id*. at 964 (Alito, J., concurring); *id*. at 955 (Sotomayor, J., concurring). Justice Sotomayor explained:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.

Id. at 955–56 (citations and quotation marks omitted); *see id*. at 964 (Alito, J., concurring).

What Justice Sotomayor observed of long-term location tracking is equally true of the mass call-tracking program. The surveillance at issue here "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).[16]

[16] The government has downplayed the sensitivity of telephony metadata, characterizing this information as "only technical data." White Paper at 15. But the government itself has recognized the sensitivity of this information in other contexts. For example, just last week, the Chairwoman of the Federal Trade Commission gave a speech underscoring the serious privacy concerns raised by the "bit-by-bit" compilation of "little data" into "enormous databases." Edith

Indeed, the program is in several respects considerably more intrusive than the location tracking that was at issue in *Jones*. The latter case involved the surveillance of a single vehicle over a twenty-eight days. The mass call-tracking program, by contrast, has involved the surveillance of every American over a period of seven years—and the government appears intent on continuing this surveillance indefinitely.[17]

In its public defense of the program, the government has relied heavily on *Smith v. Maryland*, 442 U.S. 735 (1979), in which the Supreme Court upheld the installation of a "pen register" in a criminal investigation. White Paper at 19–20. The pen register in *Smith*, however, 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. 442 U.S. at 741. It was in place for less than two days, and it was directed at a single criminal suspect. *Id.* at 737 (noting that pen register was installed after woman who had been robbed began receiving threatening and obscene phone calls from man purporting to be robber). Moreover, the information the pen register yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of innocent people. *Id*. Nothing in *Smith*—a case involving narrow

---

Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum 4 (Aug. 19, 2013), http://1.usa.gov/170P3lB; *see id*. at 4–5 ("The little data often reflects deeply personal information about individuals: the medical treatment they receive; the products and services they buy; their physical location; the websites they surf; their intimate communications with family and friends; and the list goes on.").

[17] According to the government, the scope of the program reflects the scope of the underlying investigation. *See* White Paper at 12 ("the sort of national security investigations with which Section 215 is concerned often have a remarkable breadth—spanning long periods of time, multiple geographic regions, and numerous individuals"). That the underlying investigation is so broad, however, is a factor that weighs against the government's constitutional argument. *See, e.g.*, *Keith*, 407 U.S. at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.").

surveillance directed at a specific criminal suspect over a very limited time period—remotely suggests that the Constitution allows the government's mass collection of sensitive information about every single phone call made or received by residents of the United States over a period of seven years. Notably, since *Smith* was decided in 1979, "technological advances . . . in computing, electronic data storage, and digital data mining . . . have radically increased our ability to collect, store, and analyze personal communications, including metadata." Felten Decl. ¶ 22.

Indeed, the government's reliance on *Smith* suggests that it has failed to absorb the crucial insight of *Jones*: that whether or not a particular form of surveillance constitutes a search can turn on whether the information generated through the surveillance is aggregated. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("making available . . . *such a substantial quantum of intimate information* about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society" (emphasis added and quotation marks omitted)); *id*. (stating that individuals have "a reasonable societal expectation of privacy in *the sum of* [their] public movements" (emphasis added)); *id*. at 964 (Alito, J., concurring) ("society's expectation has been that law enforcement agents and others would not—and, indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period"); *see also United States v. Knotts*, 460 U.S. 276, 284–85 (1983) (reserving question of whether the Fourth Amendment would treat dragnet location tracking differently from location tracking of a single individual). Again, the mass call-tracking program involves the aggregation of sensitive information not only over long periods of time (as was the case in *Jones*) but across hundreds of millions of people. To contend that *Smith* controls here is to

misunderstand the narrowness of the pen-register surveillance upheld in that case, the breadth of the surveillance at issue here, or both.[18]

2. The government's long-term recording and aggregation of telephony metadata is unreasonable.

i. The mass call-tracking program involves warrantless searches, which are per se unreasonable.

The mass call-tracking program authorizes warrantless searches, which "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, it authorizes the particular form of search that the authors of the Fourth Amendment found most offensive.

The program is, in reality, a general warrant for the digital age. Like a general warrant, it permits 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 authorizes 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 v. New York*, 388 U.S. 41, 59 (1967) (striking down electronic-surveillance statute that, like "general warrants," left "too much to the discretion of the officer executing the

[18] To the extent the government's argument is that individuals lack a constitutionally protected privacy interest in telephony metadata because that information has been shared with telecommunications companies, White Paper at 20, this argument, too, is mistaken. *Jones* makes clear that 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). *Jones*, moreover, is only the most recent of a line of Supreme Court cases reflecting the same principle. *See, e.g.*, *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).

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

The government has elsewhere hinted that the "special needs" doctrine excuses its failure to comply with the warrant clause. Plaintiffs will address that doctrine at greater length if the government relies upon it in this case. But even if its interest in examining the telephony metadata of suspected terrorists qualifies as a "special need," the government would still have to establish that the manner in which it pursues that interest is reasonable. *Illinois v. Lidster*, 540 U.S. 419, 426 (2004). For the reasons below, it is not.

ii. The government's long-term recording and aggregation of telephony metadata is unreasonable.

Even if the warrant requirement does not apply, the government's dragnet collection of Plaintiffs' phone records is unreasonable and, therefore, unconstitutional. Courts have insisted that the government's intrusions on privacy be precise and discriminate. *Berger*, 388 U.S. at 58. The mass call-tracking program is anything but. To pursue its limited goal of tracking the associations of a discrete number of individuals, the government has employed the most indiscriminate means possible—collecting *everyone's* records. The government has, in the words of Section 215's author, "scoop[ed] up the entire ocean to . . . catch a fish."[19]

"[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

[19] 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).

marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008). In the context of electronic surveillance, reasonableness demands that statutes have "precise and discriminate" requirements 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); *see also United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973) ("[W]e must look . . . to the totality of the circumstances and the overall impact of the statute to see if it authorizes indiscriminate and irresponsible use of electronic surveillance or if it authorizes a reasonable search under the Fourth Amendment.").

In this case, the intrusion upon Plaintiffs' privacy is substantial. The government has acquired and continues to acquire a record of every single call made to or from Plaintiffs. As explained above, those records contain a wealth of revealing information. In public statements, the government has emphasized that the mass call-tracking program does not involve the collection of the content of Americans' communications. This does not save the program. As shown above, the government need not examine the content of the communications in order to gain a "startlingly detailed" profile of each and every American. Felten Decl. ¶ 1.

The principal question in conducting the Fourth Amendment's balancing inquiry is, therefore, only whether the government's asserted interest in the mass call-tracking program justifies the blanket invasion of Plaintiffs'—and every Americans'—right to privacy. It does not.

Two Supreme Court cases are particularly instructive. In *Berger*, the Supreme Court invalidated a New York statute that authorized issuance of an "order for eavesdropping . . . upon oath or affirmation . . . that there is reasonable ground to believe that evidence of crime may be thus obtained." 388 U.S. at 43–44 & n.1. In holding that the statute violated the Fourth Amendment, the Court noted its breadth, *id.* at 55, its lack of particularity, *id.* at 55–56, the

lengthy surveillance it authorized, *id.* at 59, and the lack of a "termination date on the eavesdrop once the conversation sought [was] seized," *id.* at 59–60. These features, the Court held, allowed "indiscriminate" surveillance and permitted the "general searches" prohibited by the Fourth Amendment. *Id.* at 58–59.

Five years later, in *Keith*, the Supreme Court held unconstitutional a warrantless wiretap that the Attorney General had "deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." 407 U.S. at 300. Noting that "'reasonableness' derives content and meaning through reference to the warrant clause," *id.* at 309–10, the Court stressed that "[t]he Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised," *id.* at 317. The Court did not question the government's need to conduct electronic surveillance "to safeguard domestic security," *id.* at 315, but it asked "whether the needs of citizens for privacy and the free expression may not be better protected by requiring a warrant before such surveillance is undertaken," *id.* The Court wrote:

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment.

Id. at 320.

The mass call-tracking program lacks any of the indicia of reasonableness that the Supreme Court looked to in *Berger* and *Keith*.

First, the program authorizes surveillance that is suspicionless. Under the mass call-tracking program, the government acquires the telephone records of every customer of

Verizon—and virtually every American. The collection is not limited to specific targets. The absence of a suspicion requirement weighs heavily against the program's reasonableness. *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. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (same); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (same).

Second, the mass call-tracking program allows surveillance that is essentially indefinite. The program contains no apparent temporal limit. Rather, the government has collected every American's call records for the last seven years, and it apparently intends to continue the program indefinitely. Neither the government nor the FISC "clearly circumscribe[s] the discretion" of the government "as to when the surveillance should end." *United States v. Tortorello*, 480 F.2d 764, 774 (2d Cir. 1973). That the program has no temporal limit also weighs heavily against its reasonableness. *See United States v. Cafero*, 473 F.2d 489, 496 (3d Cir. 1973) ("Carte blanche is given no one. Executing officers are not free to intercept beyond attainment of their objective for an hour, a day, seven days, or twenty-nine days."); *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002).

Third, the program fails to limit in any way the scope and nature of phone records that the government may demand. The government simply obtains all of Plaintiffs' phone records, no matter their relevance to an ongoing investigation. In other words, the program not only fails to differentiate between individuals that the government has a legitimate interest in monitoring and those that it does not, but it draws no distinction between metadata that is relevant to an

investigation and metadata that is not. The program's lack of particularity is yet another factor that weighs heavily against its reasonableness. *Berger*, 388 U.S. at 56 (noting that the demand of particularity is "especially great" when the government targets electronic communications); *see also In re Sealed Case*, 310 F.3d at 739; *Tortorello*, 480 F.2d at 773; *Bobo*, 477 F.2d at 982; *Cafero*, 473 F.2d at 498.

Finally, the program sweeps far more broadly than necessary to achieve the government's stated interest. The government has said that its interest is in discovering the networks of particular suspected terrorists. But to achieve this interest, the government could simply collect those records relating to those individuals. The government need not collect everyone's call records in order to discover information about a discrete number of individuals.

That new technology enables the government to collect and analyze everyone's information does not mean that the Constitution permits it. This case arises because new technologies allow the government to collect, store, and analyze exponentially more information than ever before, *see* Felten Decl. ¶¶ 12, 22–24; but those capabilities are still subject to familiar constitutional limits. *See Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring). No doubt, the continuous collection of *all* phone records provides easy access, in the future, to the tiny subset of records that the government might later find a legitimate need to examine. It is not surprising that, in this digital age, intelligence officials have expressed a desire to "collect it all."[20] But, recognizing the dangers of this executive impulse to put expedience ahead of privacy, the Fourth Amendment requires that the government's searches be "carefully circumscribed." *Berger*, 388 U.S. at 58; *see also Gordon*, 236 F.2d at 919 ("[The Fourth Amendment], too, often becomes a barrier to crime investigation, as when evidence slips away because the police may not promptly

[20] Ellen Nakashima & Joby Warrick, *For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All,' Observers Say*, Wash. Post, July 14, 2013, http://wapo.st/14Nb17P.

search without a warrant. American prosecutors must learn to adjust themselves to these obstacles. The purpose of the Bill of Rights was as Madison declared, 'to oblige the government to control itself.'" (footnote omitted)). The mass call-tracking program is unreasonable because, in one fell swoop, it erodes the privacy of all Americans. It is not saved by the relative ease with which the government accomplishes that intrusion.

C. The government's long-term recording and aggregation of Plaintiffs' telephony metadata violates the First Amendment.

1. Courts apply "exacting scrutiny" to investigative practices that significantly burden First Amendment rights.

The Supreme Court has recognized that government surveillance can have a profound chilling effect on First Amendment rights. In *Keith*, the Court described these constitutional dangers in detail, writing:

> National security cases . . . often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. "Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power[.]" . . .
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation.

407 U.S. at 313–14 (internal citations omitted).

Because investigatory tools have an acute potential to stifle free association and expression, the courts have subjected such methods to "exacting scrutiny" where they substantially burden First Amendment rights. *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); *Nat'l Commodity & Barter Ass'n v. Archer*, 31 F.3d 1521, 1531 n.4 (10th Cir. 1994) (seizure of organization's membership information). This standard is a

demanding one. The government must show that its investigative methods are the least restrictive means of pursuing a compelling state interest. *See Clark*, 750 F.2d at 95. "This type of scrutiny is necessary even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct." *Elrod v. Burns*, 427 U.S. 347, 362 (1976) (quoting *Buckley v. Valeo*, 424 U.S. 1, 65 (1976) (per curiam)); *see also Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960) ("Freedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference.").

The First Amendment's protection is distinct from and often greater than that afforded by the Fourth Amendment. *See 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); *Tabbaa v. Chertoff*, 509 F.3d 89, 102–03 n.4 (2d Cir. 2007) ("[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards," than under the Fourth Amendment.); *Ealy*, 569 F.2d at 227 ("We therefore conclude that the First Amendment can serve as a limitation on the power of the grand jury to interfere with a witness' freedoms of association and expression."). Indeed, even those cases applying a Fourth Amendment analysis give First Amendment interests independent weight, requiring "scrupulous exactitude" when expressive information is at stake. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford*, 379 U.S. at 485); *see Marcus v. Search Warrants*, 367 U.S. 717 (1961).

A criminal search warrant, supported by probable cause and carefully drawn, may overcome a countervailing First Amendment interest. But as the government's demands for information become more diffuse, implicating more and more protected information on a lower

showing of relevance or need, the First Amendment calculus shifts too. Thus, courts have turned aside or limited demands for membership rolls, sweeping subpoenas for business records that would reveal the same information, and the FBI's use of mail covers to obtain the postal equivalent of "metadata." *See Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963); *Local 1814*, 667 F.2d at 269; *FEC v. Larouche Campaign, Inc.*, 817 F.2d 233, 234–35 (2d Cir. 1987) (per curiam); *Paton v. La Prade*, 469 F. Supp. 773 (D.N.J. 1978).

2. The mass call-tracking program substantially burdens Plaintiffs' First Amendment rights.

The Supreme Court has repeatedly recognized that the government's surveillance and investigatory activities can infringe on associational rights protected by the First Amendment. Thus in *NAACP v. Alabama ex rel. Patterson*, a case in which the Supreme Court invalidated an Alabama order that would have required the NAACP to disclose its membership lists, the Court wrote, "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy" may operate as "a restraint on freedom of association." 357 U.S. 449, 462 (1958). "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id.*; *see also McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341–42 (1995); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 507 (S.D.N.Y. 2004).

The government's mass call-tracking program raises precisely the same specter of associational harm by permitting the government to track every one of Plaintiffs' telephone contacts. As discussed above, 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. Many of these

communications are sensitive or confidential. *See* German Decl. ¶¶ 12–13, 23–24; Shapiro Decl. ¶ 4; Dunn Decl. ¶¶ 5–6.

The mass call-tracking program exposes all of these associational contacts to government monitoring and scrutiny. In its breadth and scope, the NSA's bulk metadata collection far exceeds the demands for membership information that produced *NAACP v. Alabama* and its progeny. *See also Bates*, 361 U.S. 516; *Gibson*, 372 U.S. 539. These seminal cases rejected government efforts to obtain basic membership rolls. By comparison, the metadata that the NSA is now gathering yields an even richer web of private associational information. It supplies a comprehensive social map of Plaintiffs' activities—reflecting the full breadth of associational ties embedded in their everyday work of public education, legal counseling, and legislative advocacy.

A corollary of this direct intrusion on Plaintiffs' associational rights is the chill it imposes on Plaintiffs' work by exposing to government scrutiny many of Plaintiffs' most sensitive contacts. Indeed, because the surveillance at issue here is so intrusive, and the information gathered by it so rich, it raises yet another concern that the Court found so troubling in *Jones*. As Justice Sotomayor there observed, generalized surveillance on this scale will inevitably have a chilling effect on First Amendment rights. *See Jones*, 132, S. Ct. at 956 (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms."). This harm amounts to a substantial and discrete First Amendment injury.

Plaintiffs regularly communicate with individuals who are themselves whistleblowers and wish to come forward with evidence of government wrongdoing, including "illegality, waste, fraud, or abuse." German Decl. ¶ 2; *see id.* ¶¶ 12–24; Shapiro Decl. ¶ 4; Dunn Decl. ¶ 6. Likewise, Plaintiffs communicate with individuals relating to potential legal representation in

suits, including the victims of government abuses, who seek legal advice and may ultimately become clients or confidential sources of information. Shapiro Decl. ¶ 4. Finally, Plaintiffs communicate with other civil society organizations across the ideological spectrum, many of whom investigate instances of government wrongdoing or criticize government policy. *Id.*

All of these individuals have an interest in maintaining the confidentiality of their communications—and all contribute centrally to Plaintiffs' First Amendment activities. *See* German Decl. ¶ 23 ("Almost universally, potential whistleblowers seeking advice from me are seeking confidentiality as to both the fact and substance of our communications."). The chilling effect of the mass call-tracking program is apparent: any person hoping to approach Plaintiffs with proof of official misconduct would be understandably wary knowing that the government receives, almost in real-time, a record of every telephone call. *See id.* ¶¶ 23–25, 28–30; *Local 1814*, 667 F.2d at 272 (recognizing that "[s]ome chilling effect . . . would be inevitable" from commission's use of subpoena power to seize payroll records (citing cases)); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (postal requirement that individuals collect communist propaganda in-person "almost certain to have a deterrent effect"). Collection of these calling records would allow the government to uncover anonymous tips or attempts by individuals to privately share sensitive information with Plaintiffs. *See* German Decl. ¶ 28; *id.* ¶¶ 15–20 (discussing the various forms of retaliation whistleblowers often face for reporting government misconduct); *McIntyre*, 514 U.S. at 341–42 ("The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."); *Talley v. California*, 362 U.S. 60, 64 (1960) (finding self-evident the fact that ordinance prohibiting anonymous handbills "would tend to restrict freedom to distribute information and thereby freedom of

expression"). In short, the mass call-tracking program aggregates in a government database sensitive information about Plaintiffs' contacts with often-wary sources. The government's call logging will inhibit and deter vital sources of information for Plaintiffs' work. *See* German Decl. ¶¶ 29–32; Shapiro Decl. ¶ 8; Dunn Decl. ¶ 9; *NAACP*, 357 U.S. at 462–63; *Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 521–23 (9th Cir. 1989).

3. The mass call-tracking program fails "exacting scrutiny" because it is an unduly broad means of seeking foreign-intelligence information.

Given these imposing burdens, the government's mass call-tracking program cannot withstand exacting scrutiny. Even "'justifiable governmental goals may not be achieved by unduly broad means having an unnecessary impact on protected rights of speech, press, or association.'" *In re Grand Jury Proceedings*, 776 F.2d at 1102–03 (quoting *Branzburg v. Hayes*, 408 U.S. 665, 680–81 (1972)); *see also In re Grand Jury Subpoena*, 701 F.2d 115, 119 (10th Cir. 1983); *Clark*, 750 F.2d 89. But this is precisely the failing of the NSA's indiscriminate collection of call records: it is broad beyond all limits, and carries with it an unreasonable and unnecessary invasion of First Amendment rights. Indeed, the program's intrusion on associational privacy and its chilling effect on protected expression are on a scale without ready comparison.

Certainly, the government has narrower methods that would serve the same ends. For one, the FBI could readily tailor its collection of telephony metadata under Section 215 to the investigation of terrorists, as the statute contemplates. *See* 50 U.S.C. § 1861. Properly anchored to a specific investigation, a demand for phone records under Section 215 could satisfy the exacting-scrutiny standard. Intelligence officials have indicated that, in 2012, the NSA queried the countless call records in its database using fewer than 300 identifiers, such as telephone numbers. *See* Ellen Nakashima, *Call Records of Fewer Than 300 People Were Searched in 2012, U.S. Says*, Wash. Post, June 15, 2013, http://wapo.st/159gMvT. While the government has

recited this figure to imply restraint, it is in reality proof that these phone records could be obtained on a case-by-case basis.

Moreover, Section 215 is not the only tool at the government's disposal; the government has other means of obtaining call records genuinely relevant to its investigative needs. *See, e.g.*, 50 U.S.C. § 1842 (FISA's "pen register" and "trap and trace" provision); 18 U.S.C. § 2709 ("national security letter" authority to demand telephony metadata "relevant to" certain investigations); 18 U.S.C. §§ 3122, 3125 ("pen register" or "trap and trace" device for criminal investigations); 18 U.S.C. § 2703(d) (court order for stored telephone records); Fed. R. Crim. P. 17(c) (subpoena); U.S. Const. amend. IV (search warrant). Rather than using any of these calibrated tools, however, government officials appear to believe that storing *all* call records is an appropriate prophylactic step given the possibility that some small subset *might* become useful in the future.

Yet members of the Senate Select Committee on Intelligence—which oversees the mass call-tracking program—have indicated that the available alternatives are every bit as effective. Shortly after the program was disclosed, Senators Ron Wyden and Mark Udall stated:

> After years of review, we believe statements that this very broad Patriot Act collection [of phone records] has been "a critical tool in protecting the nation" do not appear to hold up under close scrutiny. We remain unconvinced that the secret Patriot Act collection has actually provided any uniquely valuable intelligence. *As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans* in the way that the Patriot Act collection does.

Press Release, Office of Sen. Ron Wyden, *Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks*, June 7, 2013, http://1.usa.gov/19Q1Ng1 (emphasis added). The Senators could not be clearer: the government has more modest alternatives at its disposal, which would produce the same intelligence value while vacuuming up far fewer phone records.

Finally, the program imposes a heavy and immediate burden on Plaintiffs' First Amendment rights. In cases where investigative methods unnecessarily invade First Amendment rights, the Second Circuit has approved significant narrowing of government demands for information. In *Local 1814*, the Second Circuit found that a subpoena compelling disclosure of union members' payroll records would have an "inevitable chilling effect" on the organization's activities. 667 F.2d at 273–74. Accordingly, the Court narrowed the subpoena, whittling it down from the 450 names sought to a subset of only 45. This modification, the Second Circuit held, would "appropriately limit the impairment of longshoremen's First Amendment rights without compromising the Commission's legitimate investigative needs." *Id*. at 274; *see also Bursey v. United States*, 466 F.2d 1059, 1083 (9th Cir. 1972), *overruled in part on other grounds*, *In re Grand Jury Proceedings*, 863 F.2d 667, 669–70 (9th Cir. 1988) (affirming refusal to answer grand-jury questions on First Amendment grounds where the interrogation bore no "substantial connection to the compelling subject matter of the investigation"); *In re Grand Jury Subpoena*, 701 F.2d at 119 (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).

The mass call-tracking program fails the First Amendment test set out in every one of these cases: it reaches far beyond the government's legitimate investigative ends, while needlessly encroaching on Plaintiffs' freedom of association and expression.

II. Plaintiffs will suffer irreparable injury if preliminary relief is withheld.

Plaintiffs assert injuries flowing from the mass call-tracking program's violation of their Fourth and First Amendment rights as well as the program's violation of Section 215. The Second Circuit 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); *Public Serv. Co. of N.H. v. Town of W. Newbury*, 835 F.2d 380, 382 (1st Cir. 1987) (observing that presumption of irreparable harm is commonly applied in "cases involving alleged infringements of free speech, association, privacy, or other rights as to which temporary deprivation is viewed of such qualitative importance as to be irremediable by any subsequent relief"); *see also Covino v. Patrissi*, 967 F.2d 73, 77 (2d Cir. 1992) (applying presumption of irreparable harm in case alleging Fourth Amendment violations); *Ligon v. City of N.Y.*, No. 12 Civ. 2274, 2013 WL 628534, at *39 (S.D.N.Y. Feb. 14, 2013) (same); *Bray v. City of N.Y.*, 346 F. Supp. 2d 480, 489 (S.D.N.Y. 2004) (Pauley, J.) (finding plaintiffs' allegation of Fifth Amendment injury satisfied irreparable-harm requirement).[21]

Here, Plaintiffs would satisfy the irreparable-harm standard even if the presumption did not apply. The continuation of the surveillance at issue here would involve the continuation of the government's intrusion into Plaintiffs' sensitive associations and communications. The courts have repeatedly held that the compelled disclosure of sensitive information constitutes irreparable injury. *See Hirschfeld v. Stone*, 193 F.R.D. 175, 185–86 (S.D.N.Y. 2000) (Pauley, J.) (finding that disclosure of individual "medical histories, HIV status, substance abuse, and other intimate details of their personal lives" constitutes irreparable injury); *Slevin v. City of N.Y.*, 477

[21] The Second Circuit has modified this presumption when examining certain First Amendment injuries: irreparable harm may be presumed "[w]here a plaintiff alleges injury from a rule or regulation that directly limits speech," but "where a plaintiff alleges injury from a rule or regulation that may only potentially affect speech, the plaintiff must establish a causal link between the injunction sought and the alleged injury." *Bronx Household of Faith v. Bd. of Educ. of City of N.Y.*, 331 F.3d 342, 349–50 (2d Cir. 2003); *see Bray*, 346 F. Supp. 2d at 487–89 (distinguishing First and Fifth Amendment irreparable-harm analyses).

F. Supp. 1051, 1052 (S.D.N.Y. 1979) (finding that compelled disclosure of financial records constitutes irreparable harm); *see also Deerfield Med. Ctr. v. City of Deerfield Beach*, 661 F.2d 328, 338 (5th Cir. 1981) ("[T]he right of privacy must be carefully guarded for once an infringement has occurred it cannot be undone by monetary relief."). 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 government's queries in its call-records database compound this injury. Each time the government queries the database for *any* identifier, it analyzes Plaintiffs' calling records in order to determine whether there are matches. Thus, any query involves inspection of Plaintiffs' phone records; indeed, the government is collecting these records precisely because it wishes to sift through them for contacts within one, two, or three hops of its targets. These queries inevitably expose Plaintiffs' sensitive information and associational contacts to government scrutiny, *see supra* Parts I.B.1, I.C, and the resulting invasion of privacy is an injury that cannot be undone.

The government's searches of the mass call-tracking database work a further irreparable injury: they impose a far-reaching chill on Plaintiffs' First Amendment activities by discouraging vital sources of information from coming forward. *See supra* Part I.C. Plaintiffs, through their declarations, have demonstrated that the mass call-tracking program promises to deter whistleblowers, potential clients, and others who reasonably fear being identified by the government. The NSA's collection and searching of Plaintiff's call records is the direct cause of this chilling effect, and the ongoing damage to Plaintiffs' advocacy, public-interest litigation, and

legislative efforts cannot be remedied after the fact. *See Mullins v. City of N.Y.*, 634 F. Supp. 2d 373, 392 (S.D.N.Y. 2009).

CONCLUSION

For the foregoing reasons, the Court should grant Plaintiffs' motion and enter a preliminary injunction that, during the pendency of this suit, (i) bars Defendants from collecting Plaintiffs' call records under the mass call-tracking program, (ii) requires Defendants to quarantine all of Plaintiffs' call records already collected under the program, and (iii) prohibits Defendants from querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs.

Respectfully submitted,

/s/ Jameel Jaffer

Christopher T. Dunn (CD-3991)
Arthur N. Eisenberg (AE-2012)
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 (JJ-4653)
Alex Abdo (AA-0527)
Brett Max Kaufman (BK-2827)
Patrick Toomey (PT-1452)
Catherine Crump (CC-4067)
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

August 26, 2013