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

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

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

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

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

> 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

ARGUMENT

To justify entry of preliminary relief, Plaintiffs must show, first, that they are more likely

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

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

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

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,

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)

often sensitive or confidential; in many circumstances,

single purpose," *id.* ¶ 40, and their use can reveal a person's

The long-term recording and aggregation of telephony metadata achieves essentially the

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

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. atd, t -2(c)]dieludi p3-10(e)3j3(d)21T.24vanel0.58vmiA T8(g)4(l-2(c)], >>BDC 2.55.1(a)4(p)-10(e)3j

Indeed, the government's reliancIndc6 0 Td2e9(Td ( )Tj)4(r)3n.77 u1(time)yTd [(a a)4(ie)4(l Td [hi

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,

MTJ /TT3 1 ,BDC MBn2(n)-1g /T8uoT(on s)-1(uppl)-2(n)-1g /Taiio /Tayst /T8uoT(on s)-1(uppl)-2Fo

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*

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

Verizon—and virtually every American. The collection is not limited to specific targets. The absence of a suspicion requirement

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 indi

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—

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 readyed [(i)-2d its Tj -0.0Td [(i)-2-2(t)-2(s)

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.

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);

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,()3(C)-STJ 11.4-11.4--7(Yo)-2(r)1(k)-2(,)-2(dMC