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

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.	**DECLARATION OF STEVEN R. SHAPIRO** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF STEVEN R. SHAPIRO

I, Steven R. Shapiro, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I am the Legal Director of the American Civil Liberties Union ("ACLU"), which is a plaintiff in this case. I submit this declaration in support of the plaintiffs' motion for a preliminary injunction. I base this declaration on my personal knowledge and on information provided to me by my staff.

2. For purposes of this declaration, I use "ACLU" to refer to both the American Civil Liberties Union and the American Civil Liberties Union Foundation. The American Civil Liberties Union is a 501(c)(4) nonprofit and nonpartisan organization with approximately 500,000 members nationwide dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil-rights laws. It engages in legislative lobbying, public education, and public advocacy. The American Civil Liberties Union Foundation is a 501(c)(3) organization that provides legal representation free of charge to individuals and groups in civil-rights and civil-liberties cases. It also engages in public education and advocacy.

3. I have served as the ACLU's legal director since 1993. In that capacity, I supervise over 100 lawyers, paralegals, and support personnel who work on a wide range of issues, including—to name just a few—national security, police accountability, reproductive rights, LGBT rights, and immigrants' rights.

4. Given the controversial nature of much of the ACLU's work, the organization has a strong interest in protecting not only the content of our communications with clients, sources, and allies, but often the very fact of those communications. Many of these communications occur by telephone. For example:

- ACLU lawyers frequently place or receive telephone calls from individuals relating to potential legal representation in suits against the federal government. Among others, this includes calls from prospective whistleblowers who wish either to inform the ACLU of government misconduct or to seek legal counsel about their decision to expose that misconduct. These individuals often insist that the very fact of their communication with the ACLU be kept confidential.

- Protecting the confidentiality of a client's identity is also a paramount concern in cases where the client has been granted judicial permission to proceed pseudonymously. In such cases, any disclosure of the client's identity is generally limited by a protective order that is then subject to judicial enforcement.
- In addition, ACLU staff has had numerous conversations over the years with government sources, including members of the executive and legislative branches, in furtherance of the ACLU's advocacy efforts. The ground rules for these discussions can include a promise of confidentiality, which would be breached if it became known that the sources were talking to the ACLU, particularly if the fact or timing of those conversations would reveal the likely subject matter of the communications.
- As a nonpartisan organization, the ACLU forms alliances on discrete issues with other organizations across the ideological spectrum. The terms of the cooperation sometimes include a mutual understanding that the collaboration will be kept confidential.
- Finally, ACLU staff speak by telephone with ACLU members and donors. These conversations relate to the ACLU's work, the relationship that members and donors have with the organization, and other topics.

5. The ACLU can and does take measures to protect the confidentiality of sensitive communications from surveillance by the government or other third parties, including the use of encryption software, when deemed appropriate in the exercise of our professional judgment. Based on conversations with staff, however, my understanding is that current technology does not allow us to shield our telephony metadata from the kind of surveillance at issue here. Thus,

to our knowledge, there is no way to protect the identity of persons communicating by telephone with the ACLU through Verizon, even in circumstances where that information is especially sensitive, so long as the challenged surveillance program continues.

6. Since 2007, the ACLU has received its telephone service from Verizon Business Network Services, Inc. ("Verizon"). As of the filing of this declaration, the ACLU continues to receive its telephone service from Verizon.

7. Prior to the disclosures about the NSA's call-tracking program, the ACLU had no knowledge that its telephony metadata was being acquired and retained for years by the government. The ACLU's agreement with Verizon contains a paragraph that is labeled Customer Consent to Use of Customer Proprietary Network Information ("CPNI"), which defines 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." That provision further states, "Verizon acknowledges that it has a duty, and Customer has a right, under federal and/or state law to protect the confidentiality of Customer's CPNI." Elsewhere, the ACLU's agreement provides that "Verizon will protect the confidentiality of Customer CPNI in accordance with applicable laws, rules and regulations."

8. The NSA program at issue in this case poses a real threat to the ability of the ACLU to do its work. In my opinion, there is a genuine risk that people who would otherwise speak on the telephone with the ACLU will refrain from doing so if they believe that the government will be able to learn that they have been communicating with us. Given what we

understand about the government's surveillance program, I know of nothing we can do to protect those persons from this risk short of ceasing to speak with them on the telephone.

Steven R. Shapiro

STEVEN R. SHAPIRO

Dated: August 26, 2013

UNITED STATES DISTRICT COURT
FOR THE 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 the 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 the Director of the Federal Bureau of Investigation,

Defendants.

Case No. 13-cv-03994 (WHP)

ECF Case

DECLARATION OF MICHAEL GERMAN

I, Michael German, hereby declare and state as follows:

1. I am a resident of the Commonwealth of Virginia over the age of 18 and am principally employed in the District of Columbia. I have personal knowledge of the facts stated in this declaration.

2. I am a Senior Policy Counsel on National Security, Immigration, and Privacy at the American Civil Liberties Union ("ACLU"), where I have worked since 2006. In my work at the ACLU, I am an advocate on issues related to national security and government transparency,

and I am the ACLU's principal advocate on issues related to "whistleblowers," or individuals inside of government who wish to expose government wrongdoing (including illegality, waste, fraud, or abuse) through appropriate and legal channels. I have expertise in this area in part because I am a former federal whistleblower myself.

3. The ACLU is dedicated to defending the rights guaranteed in the Constitution and Bill of Rights, including the free-speech rights of government employees and the public's right to government information produced for public benefit and at public expense. Often, government employees and contractors are the only people in positions to disclose government waste, fraud, abuse, and illegality, and they therefore must be empowered to responsibly report these matters to the appropriate oversight officials within the executive branch—as well as to Congress, the courts and the public—without fear of reprisal. This is particularly true in the national-security context, where inappropriate or excessive use of classification can be used to hide government activities from congressional, judicial, and public oversight, and where the laws protecting whistleblowers from reprisal are weakest.

4. The ACLU lobbies in Congress and directly to executive-branch agencies to strengthen the legal protections for whistleblowers, and to provide effective due-process mechanisms for adjudicating government employees' and contractors' complaints of reprisal for having reporting waste, fraud, abuse, and illegality. The ACLU supported the Whistleblower Protections Enhancement Act of 2012, and encouraged the executive branch to promulgate Presidential Police Directive 19, which is designed to expand protections for employees of the intelligence agencies.

5. Because the ACLU is a prominent organization working on these issues, whistleblowers often contact the ACLU directly, seeking advice, representation, or both.

Because of my background as a whistleblower, many whistleblowers contact me directly to seek my guidance. In these cases, I assist prospective whistleblowers in obtaining legal advice from ACLU litigators or from public-interest groups outside the ACLU, such as the National Whistleblower Center, the Project on Government Oversight, the James Madison Project, and the Government Accountability Project, among others. I may also introduce them to congressional staff, or give them advice on which committees or members of Congress work on the issues they are concerned about or oversee the agencies in which they work. Many times I ask them if they are willing to lose their jobs in the process of bringing a problem to light. If they say "no," I often advise them that the legal protections existing today are insufficient to protect them from retaliation and they should carefully consider their decision. In some cases they do not report the misconduct as a result.

6. I sought assistance from the ACLU when I left the FBI and reported problems in the FBI counterterrorism program to Congress and the public. The ACLU also represented former FBI linguist Sibel Edmunds, who was improperly fired by the FBI after reporting problems in the agency's translation program. The ACLU of Southern California represented Federal Air Marshal Frank Terreri, who was suspended after raising concerns about policy changes that made it easier to identify Federal Air Marshals while on duty protecting air traffic. The ACLU has also assisted many other whistleblowers who have never been publicly identified.

PERSONAL WHISTLEBLOWING HISTORY

7. In June 1988, after graduating from Northwestern University Law School, I entered on duty as a Special Agent at the Federal Bureau of Investigation ("FBI"). During my career at the FBI, I had a clean disciplinary record and a consistent record of superior performance appraisals, and I received a Medal of Valor from the Los Angeles Federal Bar

Association, and a First African Methodist Episcopal Church FAME Award. In addition, through my work as an undercover agent, I successfully infiltrated domestic terrorist organizations, recovered dozens of illegal firearms and explosive devices, successfully investigated unsolved bombings, prevented acts of terrorism, and helped win criminal conviction against terrorists.

8. In 2002, I made a protected disclosure through my chain of command about management failures and violations of law in an FBI counterterrorism investigation. In particular, I learned in August 2002 that part of a meeting between subjects of an FBI investigation in which I was involved had been illegally recorded, in violation of Title III wiretap laws, by an FBI cooperating witness. On September 10, 2002, I sent a letter documenting the illegality of which I was aware up my chain of command. Almost immediately, I suffered retaliation from superior officers; later, I learned that retaliatory investigations, which were shown to be meritless, had been initiated against me because of the misconduct I reported. In November 2002, I reported the entirety of the matter to the Office of the Inspector General ("OIG") in the Department of Justice ("DOJ"). In 2004, I resigned from the FBI as a result of the retaliation I suffered after reporting the misconduct.

9. After two years of attempting to have the misconduct and deficiencies that I witnessed addressed within the FBI and DOJ, I chose to report the matter to Congress. As a result of the efforts of Senators Chuck Grassley, Arlen Specter, and Patrick Leahy, among others, the OIG ultimately released a report documenting the investigation precipitated by the illegality I reported within the FBI. The report confirms many of the allegations in my original complaint. In 2008, I testified before the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security about my whistleblowing experience within the FBI.

EXPERIENCE WITH WHISTLEBLOWERS AS ACLU POLICY COUNSEL

10. Since joining the ACLU in 2006, I have specialized in advocacy related to federal law enforcement. The primary focus of my work is the role of whistleblowers in exposing government wrongdoing, waste, fraud, and abuse. I estimate that 15 to 25 percent of my professional time is spent on this focus.

11. According to a May 2009 report by the DOJ Office of the Inspector General, *Review of the Federal Bureau of Investigation's Disciplinary System*, a survey of FBI employees indicated that 18 percent of respondents said that they "never" reported incidents of possible misconduct of which they had been made aware. Additionally, 28 percent of respondents in non-supervisory positions (GS-13 grade level or below) indicated that they "never" reported incidents of possible misconduct of which they had been made aware. The report indicated that the second-most-common reason for FBI employees failing to report misconduct incidents was fear of professional retaliation.

12. In my professional capacity, I regularly receive calls from government employees seeking advice on how to "blow the whistle" appropriately, safely, and effectively within different government agencies. In general, my relationships with these individuals are not confined to a single contact, but consist of continuing and ongoing discussions about various attempts to report misconduct and avoid retaliation that may last years at a time. The potential whistleblowers typically do not know their rights under the law, or the proper methods to report waste, fraud, abuse, or illegality within their agencies. They often do not know the responsibilities of the Inspectors General of their agencies, or how to report a complaint to those officials. Finally, they often do not know how they may bring the matter to the attention of members of Congress, and need assistance in identifying the proper committee or member to which they can report their concerns. Even after reporting through these avenues, however,

whistleblowers often need continuing assistance if, for example, the Inspectors General or congressional staff do not properly follow up to investigate the matters. Additionally, after initial reporting, whistleblowers often begin to suffer retaliation as a result of their protected disclosures. I often work with congressional staff and with staff of the Inspector General offices to address the concerns presented by federal whistleblowing.

13. In addition, sometimes individuals within the government contact me about government misconduct but cannot explain themselves fully because doing so would reveal classified information. These individuals usually are seeking safe avenues for communicating and reporting information that may be classified without committing a crime. In my experience, most of these individuals contact me because they are unaware of avenues within the government for reporting misconduct related to classified matters without exposure to adverse retaliation. In my professional experience, less than ten percent of federal-government whistleblowing involves classified information.

14. In most cases, my role in advising potential whistleblowers is to provide guidance about the available avenues for reporting government misconduct, waste, fraud, or abuse, based on my experience and expertise, as well as to assist individuals in retaining legal counsel should the individual desire it.

15. In my experience, government employees who have witnessed possible incidents of misconduct fear that they will suffer professional retaliation if they report those incidents through administrative channels.

16. In the context of whistleblowing, I am aware of various forms of professional retaliation that have occurred in the past and that commonly dissuade individuals from coming forward with information about possible government misconduct, waste, fraud, or abuse. Such

retaliation includes, but is not limited to: harassment; retaliatory investigations; internal disciplinary actions; adverse change of job duties or responsibilities; physical-location transfers; termination; and filing of criminal charges.

17. Additionally, individuals who hold security clearances from the federal government risk losing their clearance status by reporting misconduct. I am aware of numerous cases in which whistleblowers lost security clearances after reporting incidents of misconduct, or had their security clearances threatened. Employees and contractors of the FBI and intelligence agencies have little ability to defend themselves against security-clearance retaliation, and in most cases cannot maintain employment with these agencies without a clearance.

18. In my experience, one of the most dissuasive acts of professional retaliation that potential whistleblowers fear is the threat of administrative investigation. I am aware of numerous instances in which government employees chose not to report misconduct because they feared being subjected to investigations unrelated to the subject of their potential reporting. I have often heard potential whistleblowers express the concern that "no one is administratively pure," which means that no federal employee believes him- or herself to be immune to retaliatory actions if he or she were to report misconduct.

19. Typically, individuals who contact me seeking information about how to safely and legally report government misconduct are fearful that their efforts will be exposed before they decide on a course of action, and are afraid of retaliation that could damage or end their careers. Often, potential whistleblowers are perplexed and frustrated that attempts to report incidents internally are met with resistance and inaction. Many indicate that they believe there are few (and sometimes no) avenues for open communication, advice, or resources about how to

report government misconduct without exposing themselves to adverse employment consequences.

20. When contacted by individuals interested in reporting government misconduct through official channels, I regularly inform them that, based on my personal and professional experiences, simply reporting misconduct commonly leads to dismissal and other serious professional retaliation, and that they must be prepared for those potential consequences.

21. In my experience, most government whistleblowers are dedicated federal employees who have rarely found themselves in a position to challenge the government previously. Not uncommonly, individuals who contact me about potential avenues for whistleblowing are contacting the ACLU for the first time. Many times, such individuals have said to me that contacting me and my employer were actions of "last resort," because they feel that they have nowhere else to turn for guidance.

22. Many of the whistleblowers who contact me expect that their initial report of waste, fraud, abuse, or illegality will be appreciated and addressed appropriately by agency management. They are often shocked to find that they have become targets of retaliation instead, and need to report both the original complaint and a complaint of retaliation outside their agency to an Inspector General to seek protection. Unfortunately, going outside the agencies often intensifies the retaliation, and the Inspectors General are unable, and sometimes unwilling, to protect whistleblowers or properly investigate their allegations. This stage of the whistleblower process is often the most difficult for the individuals that I advise. Whistleblowers are mostly dedicated public servants who expect that the agencies they work for share their interest in serving the public welfare with honesty and integrity, and they are deeply disappointed when they find otherwise. Whistleblowers are also often ostracized by their peers, who fear that

assisting, sympathizing or even just associating with whistleblowers will harm their own careers. Whistleblowers tend to expect that their members of Congress will be interested in their stories, but often they cannot even get congressional staff to meet with them or respond to their emails. The few that do ultimately receive some public recognition for their efforts have likely already lost their jobs or their status within the agencies and, if they are members of the intelligence community, are treated as persona non grata, making them unemployable even by private contractors. Whistleblowers who choose to fight retaliation are often forced to endure years and years of litigation, at great personal expense and with little likelihood of success. These are dedicated public servants who are willing to put themselves at great risk to ensure all government agencies are held to account, but this dedication to the public interest often takes an incredible personal toll.

23. Almost universally, potential whistleblowers seeking advice from me are seeking confidentiality as to both the fact and substance of our communications. Often, individuals will contact me using personal phone numbers or email addresses in order to avoid revealing the fact of conversations with me to colleagues or superior officials within the government. Most potential whistleblowers have already raised their concerns internally, and thus understand that any public advocacy based on their accounts will be easily identified with them and could lead to adverse professional consequences.

24. My role as an advocate on whistleblower issues depends on the use of the telephone to communicate with potential whistleblowers, as opposed to other available mediums, such as email. Many of the people considering whistleblowing are extremely conflicted about the course of action to take because of their desire to serve their country by ensuring that the law is upheld, combined with their personal fears over the consequences of reporting actions that they

believe to be wrong. These conversations are emotional and difficult, and their inherent intimacy often makes them ill-suited to be conducted through electronic means. In addition, because of the sensitivity of the subject matter, most individuals who contact me about becoming a whistleblower seek to avoid creating an electronic record of their concerns and conflicts before they make the ultimate decision to come forward to report what they know.

25. In my opinion, many individuals fear that they will be discovered reaching outside a government agency to seek advice about exposing wrongdoing. These individuals are extraordinarily sensitive to the risks involved in reporting misconduct and the possibility of retaliation should they be identified as whistleblowers. As a result, I estimate that the vast majority of federal-government wrongdoing is not reported, and that most federal employees who have witnessed wrongdoing choose to "suffer in silence" as a result.

JUDGMENTS ABOUT THE EFFECT OF SECTION 215 CALL TRACKING ON THE WILLINGNESS OF FEDERAL WHISTLEBLOWERS TO CONTACT THE ACLU

26. Through news reporting and professional discussions, I am familiar with the U.S. government's bulk collection of telephony metadata under Section 215 of the Patriot Act directed at customers of Verizon Business Network Services ("Verizon").

27. I have personally reviewed a contract between the ACLU and Verizon for telephone services. From my review, I understand that Verizon is the phone-service provider for my Washington, D.C. office phone and for my cellular telephone, which is provided by my employer, the ACLU.

28. Knowledge of the frequency, duration, and timing of calls from government employees to me, or vice versa, would reveal the substance of our relationship because it would indicate that they were considering reporting government misconduct and seeking advice from me and my colleagues about how to legally go about that course of action. A small pattern of

calls between me and a federal employee would lead to a reasonable inference that the individual had knowledge of government wrongdoing, irrespective of whether the content of those calls was known.

29. Because of the professional sensitivity and risks involved for federal employees who are considering becoming whistleblowers, it is my judgment that the Section 215 call-tracking program will cause some individuals to remain silent rather than contact me or the ACLU in order to discuss their options in reporting violations. Knowledge that all of their communications with me or the ACLU are being logged by the government would present a substantial reason for individuals who are undecided about reporting violations but fearful of retaliation from reaching out for advice.

30. As a result, some individuals may decide not to seek advice from me or the ACLU about how to safely and legally report government wrongdoing, and some instances of government wrongdoing will likely go unreported.

31. Without direct contact with whistleblowers, my ability to advocate for greater protections for those who report waste, fraud, abuse, and illegality would be severely hampered. In order to design reforms that protect those conscientious employees and contractor who choose to report government wrongdoing, knowledge of how the system works, or doesn't work, is critical. Since the FBI and intelligence agencies are exempted from the Whistleblower Protection Act, internal executive-branch procedures are the only protection for employees of those agencies. As the agency mechanisms to protect whistleblowers are in a constant state of adjustment, being able to determine which practices provide relief and which create a false promise of security only comes from observing how they work for actual whistleblowers. My work for the ACLU in other national-security fields, including intelligence oversight and

classification reform, would also be severely damaged by whistleblowers' reluctance to contact me. Finally, that reluctance would hamper the ACLU's pursuit of its core missions of protecting individual victims of government misconduct and ensuring that the public receives information about that misconduct from those who have witnessed it.

32. In sum, the Section 215 call-tracking program compromises my ability to gather information and give advice that is relevant and necessary to my role and the ACLU's mission of assisting whistleblowers in safely and legally reporting government misconduct, waste, fraud, or abuse.

* * *

33. Pursuant to 28 U.S.C. § 1746, I hereby declare and state under the penalty of perjury that the foregoing is true and correct.

Date: August 26, 2013

MICHAEL GERMAN

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.	**DECLARATION OF PROFESSOR EDWARD W. FELTEN** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF PROFESSOR EDWARD W. FELTEN

I, Edward W. Felten, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. The plaintiffs in this lawsuit have challenged what they term the "mass call-tracking" program of the National Security Agency, and they have asked me to explain the sensitive nature of metadata, particularly when obtained in the aggregate. Below, I discuss how advances in technology and the proliferation of metadata-producing devices, such as phones, have produced rich metadata trails. Many details of our lives can be gleaned by examining those trails, which often yield information more easily than do the actual content of our communications.

Superimposing our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups, paints a picture that can be startlingly detailed.

2. I emphasize that I do not in this declaration pass judgment on the use of metadata analysis in the abstract. It can be an extraordinarily valuable tool. But because it can also be an unexpectedly revealing one—especially when turned to the communications of virtually everyone in the country—I write in the hope that courts will appreciate its power and control its use appropriately.

Biography

3. My name is Edward W. Felten. I am Professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy, at Princeton University.

4. I received a Bachelor of Science degree in Physics from the California Institute of Technology in 1985, a Master's degree in Computer Science and Engineering from the University of Washington in 1991, and a Ph.D. in the same field from the University of Washington in 1993. I was appointed as an Assistant Professor of Computer Science at Princeton University in 1993, and was promoted to Associate Professor in 1999 and to full Professor in 2003. In 2006, I received an additional faculty appointment to Princeton's Woodrow Wilson School of Public and International Affairs.

5. I have served as a consultant or technology advisor in the field of computer science for numerous companies, including Bell Communications Research, International Creative Technologies, Finjan Software, Sun Microsystems, FullComm and Cigital. I have authored numerous books, book chapters, journal articles, symposium articles, and other publications relating to computer science. Among my peer-reviewed publications are papers on the inference

of personal behavior from large data sets[1] and everyday objects,[2] as well as work on the extraction of supposedly protected information from personal devices.[3]

6. I have testified several times before the United States Congress on computer technology issues.

7. In 2011 and 2012, I served as the first Chief Technologist at the U.S. Federal Trade Commission ("FTC"). In that capacity, I served as a senior policy advisor to the FTC Chairman, participated in numerous civil law enforcement investigations, many of which involved privacy issues, and acted as a liaison to the technology community and industry. My privacy-related work at the FTC included participating in the creation of the FTC's major privacy report issued in March 2012,[4] as well as advising agency leadership and staff on rulemaking, law enforcement, negotiation of consent orders, and preparation of testimony.

8. Among my professional honors are memberships in the National Academy of Engineering and the American Academy of Arts and Sciences. I am also a Fellow of the Association of Computing Machinery. A copy of my curriculum vitae is attached as Exhibit 1 to this declaration.

---

[1] Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten & Vitaly Shmatikov, *"You Might Also Like:" Privacy Risks of Collaborative Filtering*, Proceedings of IEEE Symposium on Security and Privacy (May 2011), http://bit.ly/kUNh4c.

[2] William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman & Edward W. Felten, *Fingerprinting Blank Paper Using Commodity Scanners*, Proceedings of IEEE Symposium on Security and Privacy (May 2009), http://bit.ly/19AoMej.

[3] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum & Edward W. Felten, *Lest We Remember: Cold Boot Attacks on Encryption Keys*, Proceedings of USENIX Security Symposium (August 2008), http://bit.ly/13Ux38w.

[4] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), http://1.usa.gov/HbhCzA.

The Mass Call Tracking Program

9. On June 5, 2013, *The Guardian* disclosed an order issued by the Foreign Intelligence Surveillance Court ("FISC") pursuant to Section 215 of the Patriot Act (the "Verizon Order").[5] This order compelled a Verizon subsidiary, Verizon Business Network Services ("Verizon"), to produce to the National Security Agency ("NSA") on "an ongoing daily basis . . . all *call detail records* or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[6] The Director of National Intelligence subsequently acknowledged the authenticity of the Verizon Order.[7]

10. Following the disclosure of the Verizon Order, government officials indicated that the NSA's acquisition of call detail records is not limited to customers or subscribers of Verizon. In particular, the NSA's collection of this data encompasses telephone calls carried by the country's three largest phone companies: Verizon, AT&T, and Sprint.[8] Because these companies provide at least one end of the vast majority of telecommunications connectivity in the country, these

[5] Secondary Order, *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 at 2 (FISA Ct. Apr. 25, 2013), *available at* http://bit.ly/11FY393.

[6] *Id.* at 2 (emphasis added).

[7] James R. Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc.

[8] *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total.").

statements suggest that the NSA is maintaining a record of the metadata associated with nearly every telephone call originating or terminating in the United States.

11. Assuming that there are approximately 3 billion calls made every day in the United States, and also assuming conservatively that each call record takes approximately 50 bytes to store, the mass call tracking program generates approximately 140 gigabytes of data every day, or about 50 terabytes of data each year.

12. Assuming (again conservatively) that a page of text takes 2 kilobytes of storage, the program generates the equivalent of about 70 million pages of information every day, and about 25 billion pages of information every year.

13. Members of Congress have disclosed that this mass call tracking program has been in place for at least seven years, since 2006.[9]

14. On July 19, 2013, the day that the Verizon Order was set to expire, the Director of National Intelligence disclosed that the FISC had renewed the NSA's authority to collect telephony metadata in bulk.[10]

15. As noted above, the Verizon Order requires the production of "call detail records" or "telephony metadata." According to the order itself, that term encompasses, among other things, the originating and terminating telephone number and the time and duration of any call. Call detail records also typically include information about the location of the parties to the call. *See* 47 C.F.R. § 64.2003 (2012) (defining "call detail information" as "[a]ny information that

[9] *See* Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006,'* Guardian, June 6, 2013, http://bit.ly/13rfxdu; *id.* (Senator Saxby Chambliss: "This has been going on for seven years."); *see also* ST-09-0002 Working Draft – Office of the Inspector General, National Security Agency & Central Security Service (Mar. 24, 2009), http://bit.ly/14HDGuL.

[10] Press Release, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata, Office of the Director of National Intelligence (July 19, 2013), http://1.usa.gov/12ThYlT.

pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call").

16. Although this latter definition of "call detail information" includes data identifying the location where calls are made or received, I will not address mobile phone location information in this declaration. While senior intelligence officials have insisted that they have the legal authority under Section 215 to collect mobile phone location information, they have stated that the NSA is not collecting phone location information "under this program."[11]

17. The information sought from Verizon also includes "session identifying information"—*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc. These are unique numbers that identify the user or device that is making or receiving a call. Although users who want to evade surveillance can make it difficult to connect these numbers to their individual identities, for the vast majority of ordinary users these numbers can be connected to the specific identity of the user and/or device.

18. The information sought from Verizon also includes the "trunk identifier" of telephone calls. This provides information about how a call was routed through the phone network, which naturally reveals information about the location of the parties. For example, even if the government never obtains cell site location information about a call,[12] trunk identifier

[11] *See* Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, Wall St. J., June 16, 2013, http://on.wsj.com/13MnSsp; Pema Levy, *NSA FISA Metadata Surveillance: Is The Government Using Cell Phones To Gather Location Data?*, Int'l Bus. Times, Aug. 2, 2013, http://bit.ly/18WKXOV.

[12] Cell site location information ("CSLI") reflects the cell tower and antenna sector a phone is connected to when communicating with a wireless carrier's network. Most carriers log and retain CSLI for the start and end of each call made or received by a phone, and some carriers log CSLI

information revealing that a domestic call was carried by a cable from Hawaii to the mainland United States will reveal that the caller was in the state of Hawaii at the time the call was placed.

19. In the present case, government officials have stated that the NSA retains telephony metadata gathered under the Verizon Order, and others similar to it, for five years.[13] Although officials have insisted that the orders issued under the telephony metadata program do not compel the production of customers' names, it would be trivial for the government to correlate many telephone numbers with subscriber names using publicly available sources. The government also has available to it a number of legal tools to compel service providers to produce their customer's information, including their names.[14]

Metadata Is Easy to Analyze

20. Telephony metadata is easy to aggregate and analyze. Telephony metadata is, by its nature, *structured data*. Telephone numbers are standardized, and are expressed in a predictable format: In the United States, a three digit area code, followed by a three digit central office exchange code, and then a four digit subscriber number. Likewise, the time and date information

---

for text messages and data connections as well. Wireless carriers can also obtain CSLI by "pinging" a phone whenever it is turned on, even if it is not engaged in an active call. The precision of CSLI varies according to several factors, and "[f]or a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS." *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. On the Judiciary*, 113th Cong. (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://1.usa.gov/1awvgOa.

[13] *See* Letter from Ronald Weich, Assistant Attorney General, to Hon. Dianne Feinstein & Hon. Saxby Chambliss, Feb. 2, 2011, http://1.usa.gov/1cdFJ1G (enclosing *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization*); Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, Wall St. J., June 16, 2013, http://on.wsj.com/13MnSsp.

[14] *See* 18 U.S.C. § 2709 (national security letter); 18 U.S.C. § 2703(c), (d) (court order for records concerning electronic communication service).

associated with the beginning and end of each call will be stored in a predictable, standardized format.

21. By contrast, the contents of telephone calls are not structured. Some people speak English, others Spanish, French, Mandarin, or Arabic. Some people speak using street slang or in a pidgin dialect, which can be difficult for others to understand. Conversations also lack a common structure: Some people get straight to the point, others engage in lengthy small talk. Speakers have different accents, exhibit verbal stutters and disfluencies. Although automated transcription of speech has advanced, it is still a difficult and error-prone process.

22. In contrast, the structured nature of metadata makes it very easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances over the past 35 years in computing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyze personal communications, including metadata.

23. Innovations in electronic storage today permit us to maintain, cheaply and efficiently, vast amounts of data. The ability to preserve data on this scale is, by itself, an unprecedented development—making possible the maintenance of a digital history that was not previously within the easy reach of any individual, corporation, or government.

24. This newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing.

25. IBM's Analyst's Notebook and Pen-Link are two such computing tools. Both are widely used by law enforcement and intelligence agencies for this purpose.[15]

26. IBM's Analyst Notebook product is a multi-purpose intelligence analysis tool that includes specific telephony metadata analysis features, which are "routinely" used to analyze large amounts of telephony metadata.[16] IBM even offers training courses entirely focused on using Analyst's Notebook to analyze telephone call records.[17]

27. Pen-Link is a tool that is purpose-built for processing and analyzing surveillance data. It is capable of importing subscriber Call Detail Record ("CDR") data from the proprietary formats

[15] *Public Safety & Law Enforcement Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1avGItq ("IBM® i2® solutions help law enforcers to turn huge volumes of crime data into actionable insights by delivering tools for tactical lead generation, intelligence analysis, crime analysis and predictive analysis."); *see also Defense and National Security Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/18nateN ("IBM i2 solutions for military and national security organizations have been used across the world to process and analyze the vast quantities of information that they collect, to generate actionable intelligence and to share insights that help identify, predict and prevent hostile threats."); *see also* Pen-Link, *Unique Features of Pen-Link v8* at 16 (April 17, 2008), http://bit.ly/153ee9g ("Many U.S. Federal Law Enforcement and Intelligence agencies have acquired agency-wide site license contracts for the use of Pen-Link in their operations throughout the United States…Pen-Link systems are also becoming more frequently used by U.S. intelligence efforts operating in several other countries.").

[16] *Case Studies: Edith Cowan University, IBM i2 Solutions Help University Researchers Catch a Group of Would-Be Hackers*, International Business Machines (Mar. 27, 2013), http://ibm.co/13J2o36 ("Analyzing this volume of data is nothing new to many law enforcement users who routinely analyze tens of thousands of telephone records using IBM® i2® Analyst's Notebook®.").

[17] *Course Description: Telephone Analysis Using i2 Analyst's Notebook*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1d5QlB8 ("This intermediate hands-on 3-day workshop focuses on the techniques of utilizing i2 Analyst's Notebook to conduct telephone toll analysis…Learn to import volumes of call detail records from various phone carriers, analyze those records and identify clusters and patterns in the data. Using both association and temporal charts, discover how to use different layouts and more advanced tools to analyze telephonic data quickly and effectively.").

used by the major telephone companies,[18] it can import and export call data to several federal surveillance databases,[19] as well as interact with commercial providers of public records databases such as ChoicePoint and LexisNexis. Pen-Link can perform automated "call pattern analysis," which "automatically identifies instances where particular sequences of calls occur, when they occur, how often they occur, and between which numbers and names."[20] As the company notes in its own marketing materials, this feature "would help the analyst determine how many times Joe paged Steve, then Steve called Barbara, then Steve called Joe back."[21]

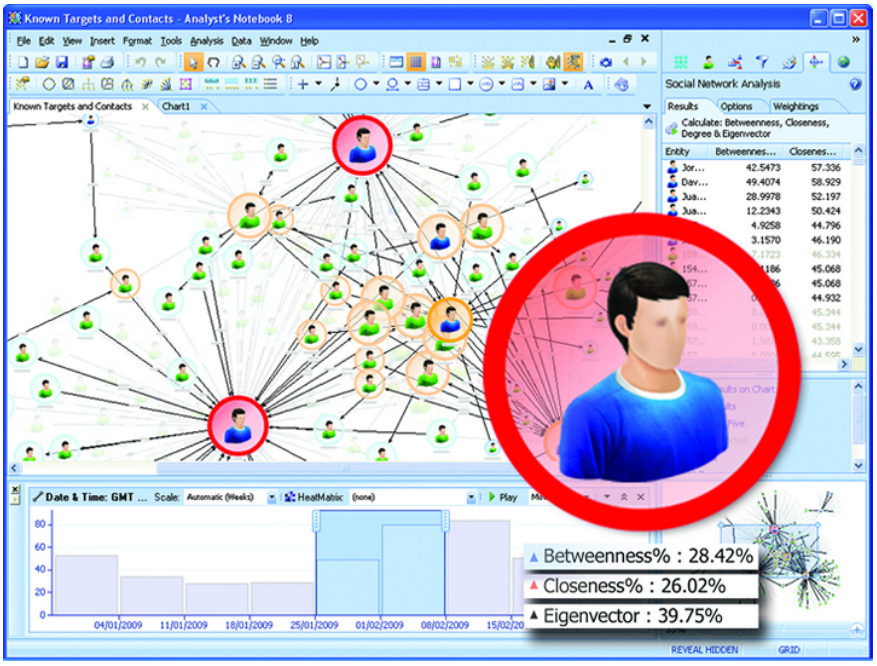

Figure 1: Screenshot of IBM's Analyst Notebook.[22]

[18] *See* Pen-Link, *Unique Features of Pen-Link v8* at 4 (Apr. 17, 2008), http://bit.ly/153ee9g (describing the capability to import 170 different data formats, used by phone companies to provide call detail records).

[19] *Id.* at 4.

[20] *Id.* at 7.

[21] *Id.*

[22] Image taken from *Data Analysis and Visualization for Effective Intelligence Analysis*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/16qT3hw.

28. The contents of calls are far more difficult to analyze in an automated fashion due to their unstructured nature. The government would first have to transcribe the calls and then determine which parts of the conversation are interesting and relevant. Assuming that a call is transcribed correctly, the government must still try to determine the meaning of the conversation: When a surveillance target is recorded saying "the package will be delivered next week," are they talking about an order they placed from an online retailer, a shipment of drugs being sent through the mail, or a terrorist attack? Parsing and interpreting such information, even when performed manually, is exceptionally difficult. To do so in an automated way, transcribing and data-mining the contents of hundreds of millions of telephone calls per day is an even more difficult task.

29. It is not surprising, then, that intelligence and law enforcement agencies often turn first to metadata. Examining metadata is generally more cost-effective than analyzing content. Of course, the government will likely still have analysts listen to every call made by the highest-value surveillance targets, but the resources available to the government do not permit it to do this for all of the calls of 300 million Americans.

The Creation of Metadata Is Unavoidable

30. As a general matter, it is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats.

31. After decades of research (much of it supported by the U.S. government), there now exist many tools that individuals and organizations can use to protect the confidentiality of their communications content. Smartphone applications are available that let individuals make encrypted telephone calls and send secure text messages.[23] Freely available software can be used

[23] Somini Sengupta, *Digital Tools to Curb Snooping,* N.Y. Times, July 17, 2013, http://nyti.ms/12JKz1s (describing RedPhone and Silent Circle).

to encrypt email messages and instant messages sent between computers, which can frustrate government surveillance efforts traditionally performed by intercepting communications as they are transmitted over the Internet.

32. However, these secure communication technologies protect only the content of the conversation and do not protect the metadata. Government agents that intercept an encrypted email may not know what was said, but they will be able to learn the email address that sent the message and the address that received it as well as the size of the message and when it was sent. Likewise, Internet metadata can reveal the parties making an encrypted audio call and the time and duration of the call, even if the voice contents of the call are beyond the reach of a wiretap.

33. There also exist security technologies specifically designed to hide metadata trails, but those technologies do not work quickly enough to allow real-time communication. The general technique for hiding the origin and destination information for an internet communication involves sending data through a series of intermediaries before it reaches the destination, thus making it more difficult for an entity such as a government agency to learn both the source and destination of the communication. (Such data is conventionally encrypted so that the intermediaries cannot capture it; and a series of intermediaries is used so that no one intermediary knows the identities of both endpoints.)

34. The most popular and well-studied of these metadata hiding systems is The Tor Project, which was originally created by the U.S. Naval Research Lab, and has since received significant funding from the State Department. One significant and widely acknowledged limitation of Tor is the noticeable delay introduced by using the tool. Web browsing conducted through Tor is much slower than through a direct connection to the Internet, as all data must be sent through a series of Tor relays, located in different parts of the world. These volunteer-run relays are

oversubscribed—that is, the demands on the few relays from hundreds of thousands of Tor users are greater than the relays can supply, leading to slowdowns due to "traffic jams" at the relay.

35. Browsing the web using Tor can be painfully slow, in some cases requiring several seconds or longer to load a page. Real-time audio and video communications require a connection with minimal delay, which Tor cannot deliver. Internet telephony and video conferencing services are simply unusable over metadata-protecting systems like Tor.

36. As a result, although individuals can use security technologies to protect the contents of their communications, there exist significant technical barriers that make it difficult, if not impossible, to hide communications metadata, particularly for real-time communications services like Internet telephony and video conferencing.

37. Over the last three decades, and especially with the widespread adoption of mobile phones in the past decade, our reliance on telecommunications has significantly increased. Mobile phones are today ubiquitous, and their use necessarily requires reliance on a service provider to transmit telephone calls, text messages, and other data to and fro. These communications inevitably produce telephony metadata, which is created whenever a person places a call. There is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether.

Telephony Metadata Reveals Content

38. Telephony metadata can be extremely revealing, both at the level of individual calls and, especially, in the aggregate.

39. Although this metadata might, on first impression, seem to be little more than "information concerning the numbers dialed,"[24] analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content.

40. In the simplest example, certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence[25] and rape,[26] including a specific hotline for rape victims in the armed services.[27] Similarly, numerous hotlines exist for people considering suicide,[28] including specific services for first responders,[29] veterans,[30] and gay and lesbian teenagers.[31] Hotlines exist for suffers of various forms of addiction, such as alcohol,[32] drugs, and gambling.[33]

---

[24] Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* 15 (Aug. 9, 2013), http://huff.to/1ey9ua5.

[25] *National Domestic Violence Hotline*, The Hotline (last visited Aug. 22, 2013), http://www.thehotline.org.

[26] *National Sexual Assault Hotline*, RAINN: Rape, Abuse & Incest National Network (last visited Aug. 22, 2013), http://www.rainn.org/get-help/national-sexual-assault-hotline.

[27] *About the Telephone Helpline*, DOD Safe Helpline (last visited Aug. 22, 2013), https://www.safehelpline.org/about-safe-helpline.

[28] *District of Columbia/Washington D.C. Suicide & Crisis Hotlines*, National Suicide Hotlines (last visited Aug. 22, 2013), http://www.suicidehotlines.com/distcolum.html.

[29] *Get Help Now! Contact us to Get Confidential Help via Phone or Email*, Safe Call Now (last visited Aug. 22, 2013), http://safecallnow.org.

[30] *About the Veterans Crisis Line*, Veterans Crisis Line (last visited Aug. 22, 2013), http://www.veteranscrisisline.net/About/AboutVeteransCrisisLine.aspx.

[31] *We Provide Crisis Intervention and Suicide Prevention for LGBTQ Youth*, The Trevor Project (last visited Aug. 22, 2013), thttp://www.thetrevorproject.org.

[32] *Alcohol Addiction Helpline*, Alcohol Hotline (last visited Aug. 22, 2013), http://www.alcoholhotline.com.

[33] *What is Problem Gambling*?, National Council on Problem Gambling (last visited Aug. 22, 2013), http://bit.ly/cyosu.

41. Similarly, inspectors general at practically every federal agency—including the NSA[34]—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud.[35] Hotlines have also been established to report hate crimes,[36] arson,[37] illegal firearms[38] and child abuse.[39] In all these cases, the metadata alone conveys a great deal about the content of the call, even without any further information.

42. The phone records indicating that someone called a sexual assault hotline or a tax fraud reporting hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private.

43. In some cases, telephony metadata can reveal information that is even more sensitive than the contents of the communication. In recent years, wireless telephone carriers have partnered with non-profit organizations in order to permit wireless subscribers to donate to charities by sending a text message from their telephones. These systems require the subscriber to send a specific text message to a special number, which will then cause the wireless carrier to add that

---

[34] Barton Gellman, *NSA Statements to the Post*, Wash. Post, Aug. 15, 2013, http://wapo.st/15LliAB.

[35] *Report Tax Fraud – Tax Fraud Hotline*, North Carolina Department of Revenue (last visited Aug. 22, 2013), http://www.dor.state.nc.us/taxes/reportfraud.html.

[36] *Report Hate Crimes*, LAMBDA GLBT Community Services (last visited Aug. 22, 2013), http://www.lambda.org/hatecr2.htm.

[37] *ATF Hotlines – Arson Hotline*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.

[38] *ATF Hotlines – Report Illegal Firearms Activity*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.

[39] *Childhelp National Child Abuse Hotline*, Childhelp (last visited Aug. 22, 2013), http://www.childhelp.org/pages/hotline-home.

donation to the subscriber's monthly telephone bill. For example, by sending the word HAITI to 90999, a wireless subscriber can donate $10 to the American Red Cross.

44. Such text message donation services have proven to be extremely popular. Today, wireless subscribers can use text messages to donate to churches,[40] to support breast cancer research,[41] and to support reproductive services organizations like Planned Parenthood.[42] Similarly, after a policy change in 2012 by the Federal Election Commission, political candidates like Barack Obama and Mitt Romney were able to raise money directly via text message.[43]

45. In all these cases, the most significant information—the recipient of the donation—is captured in the metadata, while the content of the message itself is less important. The metadata alone reveals the fact that the sender was donating money to their church, to Planned Parenthood, or to a particular political campaign.

46. Although it is difficult to summarize the sensitive information that telephony metadata about a single person can reveal, suffice it to say that it can expose an extraordinary amount about our habits and our associations. Calling patterns 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.

---

[40] *Several Ways to Give*, The Simple Church (2013), http://bit.ly/1508Mgw; *Other Ways to Give*, North Point Church (last visited Aug. 22, 2013), http://bit.ly/16S3IkO.

[41] *Donate by Text*, Susan G. Komen for the Cure (last visited Aug. 22, 2013), http://sgk.mn/19AjGP7.

[42] *Help Support a New Future for Illinois Women and Families*, Planned Parenthood of Illinois (last visited Aug. 22, 2013), http://bit.ly/1bXI2TX.

[43] Dan Eggen, *Text to 'GIVE' to Obama: President's Campaign Launches Cellphone Donation Drive*, Wash. Post, Aug. 23, 2012, http://bit.ly/16ibjCZ.

Aggregated Telephony Metadata Is Even More Revealing

47. When call metadata is aggregated and mined for information across time, it can be an even richer repository of personal and associational details.

48. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a *social graph*. By building a social graph that maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group's membership, donors, political supporters, confidential sources, and so on. Analysis of the metadata belonging to these individual callers, by moving one "hop" further out, could help to classify each one, eventually yielding a detailed breakdown of the organization's associational relationships.

49. For instance, metadata can help identify our closest relationships. Two people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway. More generally, someone you speak to once a year is less likely to be a close friend than someone you talk to once a week.

50. Even our relative power and social status can be determined by calling patterns. As *The Economist* observed in 2010, "People at the top of the office or social pecking order often receive quick callbacks, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organized (sic), such as Friday afternoons."[44]

[44] *Mining Social Networks: Untangling the Social Web*, Economist, Sep. 2, 2010, http://econ.st/9iH1P7.

51. At times, by placing multiple calls in context, metadata analysis can even reveal patterns and sensitive information that would not be discoverable by intercepting the content of an individual communication.

52. Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.

53. Likewise, although metadata revealing a single telephone call to a bookie may suggest that a surveillance target is placing a bet, analysis of metadata *over time* could reveal that the target has a gambling problem, particularly if the call records also reveal a number of calls made to payday loan services.

54. With a database of telephony metadata reaching back five years, many of these kinds of patterns will emerge once the collected phone records are subjected to even the most basic analytic techniques.

55. With an organization such as the ACLU, aggregated metadata can reveal sensitive information about the internal workings of the organization and about its external associations and affiliations. The ACLU's metadata trail reflects its relationships with its clients, its legislative contacts, its members, and the prospective whistleblowers who call the organization. Second-order analysis of the telephony metadata of the ACLU's contacts would then reveal even greater details about each of those contacts. For example, if a government employee suddenly begins contacting phone numbers associated with a number of news organizations and then the ACLU and then, perhaps, a criminal defense lawyer, that person's identity as a prospective

whistleblower could be surmised. Or, if the government studied the calling habits of the ACLU's members, it could assemble a detailed profile of the sorts of individuals who support the ACLU's mission.

56. I understand from the plaintiffs that they sometimes represent individuals in so-called "John Doe" lawsuits, where the individuals filing suit request anonymity—and are granted it by the courts—because they are juveniles or because they wish to conceal sensitive medical or psychiatric conditions. In such cases, analysis of aggregated metadata might reveal the anonymous litigant. If, for example, the lawyers in the case have only a handful of contacts in common other than mutual co-workers, and one or more of the lawyers generally call the same one of those common contacts shortly before or after hearings or deadlines in the lawsuit, this would imply the identity of the anonymous litigant. If the attorneys' calling patterns suggest more than one possible identity for the "John Doe," metadata analysis of the candidate individuals could verify the identity of the "John Doe," by correlating facts about the individuals with facts detailed in the lawsuit—for example, that he lives in a particular area (based on the area code of his phone or those of the majority of his contacts), that he has a particular job (based on calls made during work hours), that he has a particular medical condition (based on calls to medical clinics or specialists), or that he holds particular religious or political views (based on telephone donations, calls to political campaigns, or contact with religious organizations).

57. Metadata analysis could even expose litigation strategies of the plaintiffs. Review of the ACLU's telephony metadata might reveal, for example, that lawyers of the organization contacted, for example, an unusually high number of individuals registered as sex offenders in a particular state; or a seemingly random sample of parents of students of color in a racially

segregated school district; or individuals associated with a protest movement in a particular city or region.

58. In short, aggregated telephony metadata allows the government to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant.

Mass Collection of Metadata and Data-Mining Across Many Individuals

59. Advances in the area of "Big Data" over the past few decades have enabled researchers to observe even deeper patterns by mining large pools of metadata that span many telephone subscribers.

60. Researchers have studied databases of call records to analyze the communications reciprocity in relationships,[45] the differences in calling patterns between mobile and landline subscribers,[46] and the social affinity and social groups of callers.[47]

61. Researchers have discovered that individuals have unique calling patterns, regardless of which telephone they are using,[48] they have figured out how to predict the kind of device that is

[45] Lauri Kovanen, Jari Saramaki & Kimmo Kaski, *Reciprocity of Mobile Phone Calls*, Dynamics of Socio-Economic Systems (Feb. 3, 2010), http://arxiv.org/pdf/1002.0763.pdf.

[46] Heath Hohwald, Enrique Frias-Martinez & Nuria Oliver, *User Modeling for Telecommunication Applications: Experiences and Practical Implications* 8, (Data Mining and User Modeling Group, Telefonica Research, 2013), http://bit.ly/1d7WkUU ("Interestingly, Monday is the day with most calls for landline users, while Friday is the day with most calls for mobile users. . . Mobile users spend less time on the phone than landline users.").

[47] Sara Motahari, Ole J. Mengshoel, Phyllis Reuther, Sandeep Appala, Luca Zoia & Jay Shah, *The Impact of Social Affinity on Phone Calling Patterns: Categorizing Social Ties from Call Data Records*, The 6th SNA-KDD Workshop (Aug. 12, 2012), http://b.gatech.edu/1d6i4RY.

making the calls (a telephone or a fax machine),[49] developed algorithms capable of predicting whether the phone line is used by a business or for personal use,[50] identified callers by social group (workers, commuters, and students) based on their calling patterns,[51] and even estimated the personality traits of individual subscribers.[52]

62. The work of these researchers suggests that the power of metadata analysis and its potential impact upon the privacy of individuals increases with the scale of the data collected and analyzed. It is only through access to massive datasets that researchers have been able to identify or infer new and previously private facts about the individuals whose calling records make up the telephone databases. Just as multiple calls by the same person reveal more than a single call, so too does a database containing calling data about millions of people reveal more information about the individuals contained within it than a database with calling data about just one person. As such, a universal database containing records about all Americans' communications will reveal vastly more information, including new observable facts not currently known to the

---

[48] Corrina Cortes, Daryl Pregibon & Chris Volinsky, *Communities of Interest*, AT&T Shannon Research Labs, http://www.research.att.com/~volinsky/papers/portugal.ps.

[49] Haim Kaplan, Maria Strauss & Mario Szegedy, *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, AT&T Labs, http://bit.ly/19Aa8Ua.

[50] Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research, http://bit.ly/153pMcI.

[51] Richard A. Becker, Ramon Caceres, Karrie Hanson, Ji Meng Loh, Simon Urbanek, Alexander Varshavsky & Chris Volinsky, *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, AT&T Labs-Research, http://soc.att.com/16jmKdz.

[52] Rodrigo de Oliveira, Alexandros Karatzoglou, Pedro Concejero, Ana Armenta & Nuria Oliver, *Towards a Psychographic User Model from Mobile Phone Usage*, CHI 2011 Work-in-Progress (May 7–12, 2011), http://bit.ly/1f51mOy; *see also* Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic & Alex (Sandy) Pentland, *Predicting People Personality Using Novel Mobile Phone-Based Metrics*. Social Computing, Behavioral-Cultural Modeling and Prediction (2013), http://bit.ly/1867vWU.

research community, because no researcher has access to the kind of dataset that the government is presumed to have.

63. A common theme is seen in many of these examples of "big data" analysis of metadata. The analyst uses metadata about many individuals to discover patterns of behavior that are indicative of some attribute of an individual. The analyst can then apply these patterns to the metadata of an individual user, to infer the likely attributes of that user. In this way, the effect of collecting metadata about one individual is magnified when information is collected across the whole population.

64. 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. Mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals.

Edward W. Felten

Dated: August 23, 2013

EXHIBIT 1

Edward W. Felten

Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University
Sherrerd Hall, Room 302
Princeton NJ 08544
(609) 258-5906
(609) 964-1855 fax
felten@cs.princeton.edu

Education

Ph.D. in Computer Science and Engineering, University of Washington, 1993.
Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.
M.S. in Computer Science and Engineering, University of Washington, 1991.
B.S. in Physics, with Honors, California Institute of Technology, 1985.

Employment

Professor of Computer Science and Public Affairs, Princeton University, 2006-present.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.
Associate Professor of Computer Science, Princeton University, 1999-2003.
Assistant Professor of Computer Science, Princeton University, 1993-99.
Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-present
U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.
U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..
Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.
Certus Ltd.: consultant in product design and analysis, 2000-2002.
Cigital Inc.: Technical Advisory Board member, 2000-2007.

Cloakware Ltd.: Technical Advisory Board member, 2000-2003.
Propel.com: Technical Advisory Board member, 2000-2002.
NetCertainty.com: Technical Advisory Board member, 1999-2002.
FullComm LLC: Scientific Advisory Board member, 1999-2001.
Sun Microsystems: Java Security Advisory Board member, 1997-2001.
Finjan Software: Technical Advisory Board member, 1997-2002.
International Creative Technologies: consultant in product design and analysis, 1997-98.
Bell Communications Research: consultant in computer security research, 1996-97.

Honors and Awards

National Academy of Engineering, 2013.
American Academy of Arts and Sciences, 2011
ACM Fellow, 2007.
EFF Pioneer Award, 2005.
Scientific American Fifty Award, 2003.
Alfred P. Sloan Fellowship, 1997.
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.
NSF National Young Investigator award, 1994.
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.
Best Paper award, 1995 ACM SIGMETRICS Conference.
AT&T Ph.D. Fellowship, 1991-93.
Mercury Seven Foundation Fellowship, 1991-93.

Research Interests

Information security. Privacy. Technology law and policy. Internet software. Intellectual property policy. Using technology to improve government. Operating systems. Interaction of security with programming languages and operating systems. Distributed computing. Parallel computing architecture and software.

Professional Service

Professional Societies and Advisory Groups

ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-present.
DARPA Privacy Panel, 2010-2012.
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.
National Academies study committee on Air Force Information Science and Technology Research, 2004-present.
Electronic Frontier Foundation, Advisory Board, 2004-2007.
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.
DARPA Information Science and Technology (ISAT) study group, 2002-2004.
Co-chair, ISAT study committee on "Reconciling Security with Privacy," 2001-2002.
National Academy study committee on Foundations of Computer Science, 2001-2004.

Program Committees

World Wide Web Conference, 2006.
USENIX General Conference, 2004.
Workshop on Foundations of Computer Security, 2003.
ACM Workshop on Digital Rights Management, 2001.
ACM Conference on Computer and Communications Security, 2001.
ACM Conference on Electronic Commerce, 2001.
Workshop on Security and Privacy in Digital Rights Management, 2001.
Internet Society Symposium on Network and Distributed System Security, 2001.
IEEE Symposium on Security and Privacy, 2000.
USENIX Technical Conference, 2000.
USENIX Windows Systems Conference, 2000.
Internet Society Symposium on Network and Distributed System Security, 2000.
IEEE Symposium on Security and Privacy, 1998.
ACM Conference on Computer and Communications Security, 1998.
USENIX Security Symposium, 1998.
USENIX Technical Conference, 1998.
Symposium on Operating Systems Design and Implementation, 1996.

Boards

Electronic Frontier Foundation, Board of Directors, 2007-2010.
DARPA Information Science and Technology study board, 2001-2003.
Cigital Inc.: Technical Advisory Board.
Sun Microsystems, Java Security Advisory Council.
Cloakware Ltd.: Technical Advisory Board.
Propel.com: Technical Advisory Board.
Finjan Software: Technical Advisory Board.
Netcertainty: Technical Advisory Board.
FullComm LLC: Scientific Advisory Board.

University and Departmental Service

Committee on Online Courses, 2012-present
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
- Member, Executive Committee
- Co-Chair, Interactions with Industry area.
- Co-Chair, Engineering, Policy, and Society area.

Faculty Advisory Committee on Policy, 2002-present.
Council of the Princeton University Community, 2002-present (Executive Committee)
Faculty Advisory Committee on Athletics, 1998-2000.

Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)
Faculty-Student Committee on Discipline, 1996-98.
Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

Students Advised

Ph.D. Advisees:

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy.
Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud.
Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality.
William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.
Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.
J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Assistant Professor of Computer Science, University of Michigan.
Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.
Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Assistant Professor of Computer Science, University of Texas.
Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.
Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.
Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.
Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.
Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Associate Professor of Computer Science, Rice University.

Significant Advisory Role:

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Program Manager at DARPA.
Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Staff technologist at Facedbook.
Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Research Scientist, School of Computer Science, Carnegie Mellon University.

Publications

Books and Book Chapters

[1] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In Open Government, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.

[2] Securing Java: Getting Down to Business with Mobile Code. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.

[3] Java Security: Web Browsers and Beyond. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.

[4] Java Security: Hostile Applets, Holes and Antidotes. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996

[5] Dynamic Tree Searching. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

Journal Articles

[6] Government Data and the Invisible Hand. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. Yale Journal of Law and Technology, vol. 11, 2009.

[7] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Software – Practice and Experience, 33:461-480, 2003.

[8] The Digital Millennium Copyright Act and its Legacy: A View from the Trenches. Illinois Journal of Law, Technology and Policy, Fall 2002.

[9] The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. ACM Transactions on Software Engineering and Methodology, 9:4, October 2000.

[10] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. IEEE Software, 17(5), Sept./Oct. 2000.

[11] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. IEEE Micro 17(1):8-18, February 1997.

[12] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. IEEE Transactions on Parallel and Distributed Computing, February 1997.

[13] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. ACM Transactions on Computer Systems, Nov 1996.

[14] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. IEEE Micro, 15(1):21-28, February 1995.

Selected Symposium Articles

[15] Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2012.

[16] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2011

[17] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.

[18] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.

[19] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.

[20] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17th Network and Distributed System Security Symposium, 2010.

[21] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham, Proc. Electronic Voting Technology Workshop, 2009.

[22] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.

[23] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.

[24] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.

[25] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.

[26] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.

[27] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[28] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[29] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

[30] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14th World Wide Web Conference, 2005.

[31] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.

[32] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3rd Workshop on Privacy in Electronic Society. November 2004.

[33] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.

[34] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.

[35] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11th USENIX Security Symposium, August 2002.

[36] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)

[37] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.

[38] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.

[39] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.

[40] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.

[41] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.

[42] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.

[43] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

[44] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.

[45] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.

[46] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20th National Information Systems Security Conference, Oct. 1997.

[47] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.

[48] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)

[49] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.

[50] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.

[51] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.

[52] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.

[53] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.

[54] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[55] Improving Release-Consistent Shared Virtual Memory using Automatic Update . Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[56] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

[57] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.

[58] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.

[59] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.

[60] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.

[61] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.

[62] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.

[63] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.

[64] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

Selected Other Publications

[65] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. American Scientist, 97:4. July/August 2009.

[66] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.

[67] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.

[68] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy,* Jan./Feb. 2006.

[69] Inside RISKS: DRM and Public Policy. Edward W. Felten. Communications of the ACM, 48:7, July 2005.

[70] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. IEEE Security and Privacy, May 2003.

[71] A Skeptical View of DRM and Fair Use. Edward W. Felten. Communications of the ACM 46(4):56-61, April 2003.

[72] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.

[73] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.

[74] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.

[75] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.

[76] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.

[77] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.

[78] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.

[79] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.

[80] Inside RISKS: Webware Security. Edward W. Felten. Communications of the ACM, 40(4):130, 1997.

[81] Simplifying Distributed File Systems Using a Shared Logical Disk.Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

[82] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.

[83] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.

[84] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.

[85] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.

[86] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.

[87] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.

[88] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.

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.	**DECLARATION OF CHRISTOPHER DUNN** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF CHRISTOPHER DUNN

I, Christopher Dunn, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I am the Associate Legal Director of the New York Civil Liberties Union, which is a plaintiff in this case. I submit this declaration in support of the plaintiffs' motion for a preliminary injunction. I base this declaration on my personal knowledge and on information provided to me by NYCLU staff.

2. Founded in 1951 as the New York affiliate of the American Civil Liberties Union ("ACLU"), the New York Civil Liberties Union is a 501(c)(4) non-profit, nonpartisan organization that engages in public education and lobbying with respect to constitutional principles of liberty and equality. The NYCLU has more than 40,000 members throughout New York State. It is incorporated in New York and has its principal place of business in New York City. The New York Civil Liberties Union Foundation is a 501(c)(3) non-profit organization that represents clients in lawsuits seeking to advance civil liberties and civil rights, while also engaging in advocacy and public education around these issues. It is incorporated in Delaware and has its principal place of business in New York City. For purposes of this declaration, I use "NYCLU" to refer to both the New York Civil Liberties Union and the New York Civil Liberties Union Foundation.

3. I have served as the NYCLU's Associate Legal Director since 2002. The NYCLU's legal department has approximately 15 lawyers, paralegals, and support personnel who work on a wide range of issues, including—to name just a few—national security, police accountability, freedom of speech, freedom of religion, voting rights, reproductive rights, race, gender and sexual orientation discrimination. The NYCLU frequently co-counsels with the ACLU in national security cases brought in the Southern District of New York. *See, e.g.*, *Clapper v. Amnesty*, 133 S. Ct. 1138 (2013); *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2009).

4. I am familiar with the declaration being filed in this matter by ACLU Legal Director Steven Shapiro. Given the overlap of the work of the NYCLU and ACLU, many of the concerns expressed by Mr. Shapiro on behalf of the ACLU are shared by the NYCLU.

5. NYCLU legal staff frequently place or receive telephone calls from individuals relating to potential legal representation in suits against state and local governments and sometimes against the federal government. Often, the mere fact that the NYCLU has communicated with these individuals is sensitive. For example, the NYCLU has received calls from employees of the New York City Police Department ("NYPD") who wished to inform the NYCLU of misconduct within the NYPD. In virtually all of those calls, police employees have insisted that the very fact of their speaking with the NYCLU be kept strictly confidential.

6. NYCLU legal staff often speak on the telephone to communicate with government and industry whistleblowers, legislators and their staffs, and possible litigation or advocacy partners who consider the confidentiality of their associations and communications with the NYCLU essential to their willingness to speak with us. From time to time, NYCLU staff also speak by telephone with the organization's members.

7. The NYCLU was a customer of Verizon Business Network Services ("Verizon") until early April 2013. Until then, Verizon provided the NYCLU's wired communications, including its landlines.

8. Prior to the disclosures about the NSA mass call-tracking program, the NYCLU believed that its telephone communications through Verizon were secure from routine government monitoring.

9. The NSA program at issue in this case poses a substantial threat to the ability of the NYCLU to do its work, which includes public advocacy on controversial subjects, the representation of clients in litigation or in anticipation of litigation, and efforts to lobby elected local, state, and federal officials. I am confident that there are persons who speak on the

telephone with our legal staff who will refrain from doing so if they believe that the government will be able to learn of the fact that they have communicated with us. The privacy of such communication is clearly compromised by the government's mass call-tracking program. The preliminary injunctive relief requested in this motion is necessary to restore a sense of comfort and confidence in the confidentiality of the various sensitive telephonic communications that we undertake.

CHRISTOPHER DUNN

Dated: August 26, 2013
New York, N.Y.