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

PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

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. This surveillance continues, with the NSA collecting new records every day. Today, the ACLU's lawyers made calls to clients, witnesses, reporters, legislative staff, and whistleblowers. The NSA will soon have a record of each of these calls—perhaps it already does.

Plaintiffs filed suit on June 11, 2013, contending that the NSA's 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 all of Plaintiffs' call records it has already collected.

The government asks the Court to dismiss Plaintiffs' suit, arguing that Plaintiffs lack standing to pursue their claims, that their statutory claim is impliedly precluded, and that the Complaint does not state a plausible claim for relief. These arguments are without merit.

Plaintiffs have standing. The call records contain private information about Plaintiffs and their associations. Under both the Fourth and First Amendments, the collection of that information is, by itself, a direct and immediate injury to Plaintiffs' privacy interests. Plaintiffs suffer a further injury in the chilling effect that the mass call-tracking program has on key contacts and sources for their legal and advocacy work.

On the merits of each of their claims, Plaintiffs show a plausible entitlement to relief. The program is ostensibly based on Section 215 of the Patriot Act, but it disregards that provision's core requirements, adopting a strained and limitless definition of "relevance" that was never intended or ratified by any Congress. In arguing that Plaintiffs' Section 215 claim is impliedly precluded, the government fails to overcome the Administrative Procedure Act's strong presumption in favor of judicial review, which entitles Plaintiffs to pursue their statutory claim in

this Court, alongside their constitutional claims. The program violates the Fourth Amendment because the NSA's collection of Plaintiffs' call records constitutes a search and is both warrantless and unreasonable. And it violates the First Amendment because it substantially and unjustifiably burdens Plaintiffs' associational rights when narrower methods would accommodate the government's interests. The Court should deny Defendants' motion.

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 years of in-depth congressional investigation revealing that the executive branch had engaged in widespread warrantless surveillance of U.S. citizens "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. 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.). 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 obtain an order requiring the production of "any tangible things" upon a

[1] The "Patriot Act" is the name commonly used for 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).

"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).

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 for a three-month period. Compl. ¶ 30. Telephony metadata includes, for each phone call, the originating and terminating telephone number as well as the call's time and duration. Compl. ¶ 35. The FISC has since renewed the Secondary Order. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things From [Redacted]* at 15–16, No. BR 13-109 (FISA Ct. Aug. 29, 2013) ("2013 FISC Opinion").

The government has disclosed that the Secondary Order belongs to a broader NSA 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. Compl. ¶¶ 1, 33. The Secondary Order was issued pursuant to a "Primary Order" that sets out procedures the NSA must follow to "query" telephony metadata collected under the program. *See* Gov't Br. 5 & n.1; Gov't Br. Ex. 2 (Primary Order).

The Primary Order explains how the government analyzes information housed in the massive database assembled by the call-tracking program. Specifically, the order indicates 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; *see* Gov't Br. 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. *See* Gov't Br. 5–6 (discussing "contact-chaining" analysis); *Oversight of the Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. at 1:39:20–1:41:10 (2013), http://cs.pn/1bpUHRJ ("HJC Hearing") (testimony of John C. Inglis, NSA Deputy Director). 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 a target would have accessed records concerning more than two million people.

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 services. Compl. ¶¶ 3, 28. Until early April 2013, Plaintiffs New York Civil Liberties Union and New York Civil Liberties Union Foundation (together, "NYCLU") were also customers of Verizon. *Id.* ¶¶ 3, 29. As current and former Verizon customers, Plaintiffs have had their telephony metadata collected in bulk pursuant to the Secondary Order and its predecessors. *Id.* ¶¶ 3, 35. Its collection of Plaintiffs' telephony metadata continues "on an ongoing daily basis." *Id.* ¶ 30 (quoting Secondary Order at 2).

ARGUMENT

On a motion to dismiss, the Court must accept as true all the factual allegations in the Complaint and construe all reasonable inferences therefrom in the light most favorable to Plaintiffs. *See Roth v. Jennings*, 489 F.3d 499, 501 (2d Cir. 2007). Through this lens, the Court must determine whether the well-pleaded factual allegations "plausibly give rise to an entitlement to relief." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). As the Second Circuit has emphasized, the plausibility standard "does not impose a probability requirement at the pleading stage," but simply asks whether the Complaint presents sufficient facts to "permit a reasonable inference" that the Plaintiff has stated a claim. *Anderson News, L.L.C. v. Am. Media, Inc.*, 680 F.3d 162, 182–84 (2d Cir. 2012) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)).

I. Plaintiffs have established their standing to sue.

Plaintiffs have standing under Article III. They have suffered an injury because they "are current VBNS subscribers whose communications have already been monitored by the government under the VBNS order and whose communications continue to be monitored." Compl. ¶ 3. The injury is plainly traceable to the conduct they challenge—that is, to the government's collection of their call records. And the injury would be redressed by the relief they seek—principally, an injunction against the mass call-tracking program.

The government argues that Plaintiffs lack standing because they cannot prove that the government will use Plaintiffs' call "records to identify persons with whom Plaintiffs speak," or that "others might refrain from communicating with Plaintiffs because they fear disclosure of their associations with Plaintiffs." Gov't Br. 11, 13. These arguments are misguided.

As an initial matter, the government mischaracterizes the Complaint. Plaintiffs' challenge is not limited to the NSA's use of Plaintiffs' call records after collecting them but is also directed

at the government's collection of those records in the first place. *See, e.g.*, Compl. ¶ 1 ("The practice is akin to snatching every American's address book—with annotations detailing whom we spoke to, when we talked, for how long, and from where."); *id.* ¶ 35. The collection of Plaintiffs' call records is *itself* an injury sufficient for Article III; indeed, as the Complaint makes clear, the collection of Plaintiffs' call records constitutes a gross invasion of their privacy.

Even if the relevant question were whether the NSA had reviewed Plaintiffs' records, the government has acknowledged that it has done so. The Primary Order indicates that every time the NSA queries the call-records database, it reviews everyone's records—Plaintiffs' among them—to determine whether they, their contacts, or their contacts' contacts are connected to a phone number that the NSA deems suspicious. *See* Primary Order at 6–7, 11. Government officials have stated that the NSA conducted hundreds of these queries in 2012 alone. *See* HJC Hearing at 29:33–36:00 (testimony of John C. Inglis, NSA Deputy Director).[2]

The government's reliance on *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), is misplaced. In that case, which involved a constitutional challenge to the FISA Amendments Act of 2008, a divided Supreme Court held that the plaintiffs lacked standing. *See id.* at 1142–43. The Court reached that conclusion, however, not because the plaintiffs failed to demonstrate that their communications had been "retrieved" from government databases, Gov't Br. 12, but because the plaintiffs failed to demonstrate that their communications had been collected at all. *Amnesty*, 133 S. Ct. at 1147–50. Indeed, in *Amnesty* the government did not

[2] The government's theory appears to be that it has not examined Plaintiffs' call records unless the NSA finds, after querying its database, that Plaintiffs are linked to a targeted phone number. That does not make sense. A person whose luggage is inspected has been searched even if the inspection turns up no contraband. A person whose home is subjected to thermal-imaging has been searched even if the scan does not show that the person is growing marijuana. *Cf. Kyllo v. United States*, 533 U.S. 27 (2001). Whether a search has occurred does not turn on whether the search produces information that the government regards as useful or incriminating.

dispute that the plaintiffs would have standing if they could show that the government had collected their communications. It is only now, confronted with plaintiffs who make this showing, that the government argues that mere collection is not enough.

To the extent the government's argument is that the "mere" collection of Plaintiffs' call records does not inflict an injury, that argument goes to whether Plaintiffs have a reasonable expectation of privacy—that is, to the merits—not standing. As the Supreme Court has observed, the definition of Fourth Amendment rights "is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *accord Rakas v. Illinois*, 439 U.S. 128, 139 (1978). In any event, there can be no dispute that the bulk collection of Plaintiffs' call records gives them the stake in this litigation that Article III requires. Courts frequently analyze third-party challenges to records requests at the merits stage, rather than as a question of standing. *See, e.g.*, *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 270 (2d Cir. 1981); *Koch v. Greenberg*, No. 07 Civ. 9600, 2009 WL 2143634, at *3 n.1 (S.D.N.Y. July 14, 2009).

The arguments that the government directs at Plaintiffs' First Amendment claim are also incorrect. The government contends that the Complaint fails to allege with sufficient specificity that the NSA's surveillance might discourage third parties from communicating with Plaintiffs. Gov't Br. 14. But Plaintiffs' First Amendment claim asserts a direct intrusion into their associational privacy, not just a chilling effect. Compl. ¶¶ 3, 35; *cf. FEC v. LaRouche Campaign, Inc.*, 644 F. Supp. 120, 122 (S.D.N.Y. 1986) ("[T]he Supreme Court has held that the compelled disclosure of an individual's affiliation with an organization may, standing alone, constitute a serious intrusion on the First Amendment right to privacy of association and belief."), *aff'd*, 817 F.2d 233 (2d Cir. 1987) (per curiam). As above, this intrusion and the resulting injury is

complete when the government collects Plaintiffs' call records—regardless whether the surveillance ultimately dissuades any third party from communicating with them.

Plaintiffs suffer a further, discrete injury because of the program's chilling effect on their key contacts and sources. The government argues that Plaintiffs' Complaint does not describe this injury with sufficient specificity, but to survive a motion to dismiss Plaintiffs need not supply detailed factual allegations. Their obligation, rather, is to provide a "short and plain statement of the claim showing that the pleader is entitled to relief" in order to "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 555 (quotation marks omitted). Plaintiffs' Complaint satisfies this requirement. It alleges that the government's monitoring of call records intrudes into Plaintiffs' private associations. Compl. ¶¶ 3, 24–27. And it alleges that this monitoring will dissuade crucial contacts from associating with Plaintiffs, identifying the categories of contacts most likely to experience this chill. Compl. ¶¶ 3, 26–27, 35. The government seems to believe that there is something implausible about the notion that the NSA's surveillance might chill lawful expression and association, but "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association." *NAACP v. Alabama*, 357 U.S. 449, 462 (1958); *see also Local 1814*, 667 F.2d at 273; *Talley v. California*, 362 U.S. 60, 64 (1960).

II. Plaintiffs have stated a claim under the Administrative Procedure Act.

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. The

notion that detailed information about every phone call made by a resident of the United States over seven years could be "relevant to an authorized investigation" flouts precedent and common sense, as well as the larger statutory scheme. The government's construction of Section 215 is impossible to reconcile with other statutory provisions, including provisions relating to foreign-intelligence surveillance and the collection of call records in law-enforcement investigations. The government contends that Congress has ratified its radical construction of Section 215, but it would transform the legislative-ratification doctrine beyond recognition to hold that Congress impliedly ratified a legal theory that was developed in secret, never discussed publicly, and of which Congress was never fully informed.

1. The call records collected under the program are not "relevant to an authorized investigation."

The government argues that by using the term "relevant," Congress meant to incorporate into Section 215 the standard used by courts in evaluating the lawfulness of grand-jury subpoenas and similar instruments. *See* Gov't Br. 23. *But see infra* 11–15. Even if that understanding is correct, courts evaluating such instruments have given "relevance" a broad compass but by no means an unlimited one. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts have routinely narrowed or quashed subpoenas that would have required the production of records that were not sufficiently connected to the purpose of the underlying investigation. *See, e.g.*, *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (Friendly, J.) (narrowing grand-jury subpoena because it improperly demanded the contents of multiple filing cabinets "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period"); *In re Grand Jury*

Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 12–13 (S.D.N.Y. 1994) (Mukasey, J.); *see also, e.g.*, *In re Six Grand Jury Witnesses*, 979 F.2d 939, 943 (2d Cir. 1992).

Thus "relevance" is a term of art, but its technical definition is consistent with common usage. One thing is relevant to another if there is a demonstrably close connection between them. *See Oxford American Dictionary* 1474 (3d ed. 2010) (defining "relevance" as "the state of being closely connected or appropriate to the matter in hand"); *Webster's Collegiate Dictionary* 1051 (11th ed. 2012) (defining "relevance" as "having significant and demonstrable bearing on the matter at hand").

In support of its argument that the relevance standard does not preclude it from collecting vast quantities of concededly irrelevant information, the government points to cases in which courts sanctioned subpoenas that sought "entire repositories of records." Gov't Br. 22. These cases, however, do not go as far as the government suggests. Most of them stand for the unremarkable proposition that courts will not automatically quash subpoenas merely because they seek *some* concededly irrelevant records among other plainly relevant ones.[3] Others simply indicate that a subpoena may cover a large volume of relevant records.[4] Still others involve records whose relevance was either stipulated or undisputed.[5]

None of the cases cited by the government involved a subpoena that swept remotely as broadly as the mass call-tracking program does. Indeed, the government concedes as much. Gov't Br. 24 (acknowledging that the case law "does not involve data acquisition on the scale of

[3] *See FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987); *Carrillo Huettel, LLP v. SEC*, No. 11cv65, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011); *Goshawk Dedicated, Ltd. v. Am. Viatical Servs., LLC*, No. 1:05-CV-2343, 2007 WL 3492762, at *1 (N.D. Ga. Nov. 5, 2007).

[4] *See In re Subpoena Duces Tecum*, 228 F.3d 341, 350–51 (4th Cir. 2000).

[5] *See In re Adelphia Commc'ns Corp.*, 338 B.R. 546, 551–52 (Bankr. S.D.N.Y. 2005); *Medtronic Sofamor Danek, Inc. v. Michelson*, 229 F.R.D. 550, 552 (W.D. Tenn. 2003).

the telephony metadata collection authorized by the FISC"). If the subpoena cases establish anything, it is that the relevance standard precludes the kind of fishing expedition the government is conducting here. *See, e.g.*, *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))); *see also, e.g.*, *United States v. Reed*, 726 F.2d 570, 577 (9th Cir. 1994) (A subpoena under Rule 17(c) does not "allow a blind fishing expedition seeking unknown evidence." (quotation marks omitted)).

Ultimately, the government does not try to establish that the call records are relevant in any conventional sense. *See* Gov't Br. 24; *see also* 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 ("[M]ost of the records in the dataset are not associated with terrorist activity."). Instead, it argues that the statute authorizes it to collect the call records because those records are "necessary to the application of investigative techniques that will advance [an investigation's] purpose." Gov't Br. 24. It is not entirely clear what the government means by this. Does the statute allow the government to collect DNA from everyone in order to narrow, by process of elimination, the pool of suspects who might have committed a particular crime? Does the statute allow the government to compel a university to turn over technology that would allow more efficient or revealing analysis?

There is no need to explore the far reaches of the government's theory, however, because it is plain that the theory has no foundation in the text of Section 215. The text of the statute is no broader than the text of many other compulsory-disclosure statutes. *See, e.g.*, 18 U.S.C.

§ 2709(b)(1) (authorizing FBI to compel production of toll-billing and other records "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities"); 20 U.S.C. § 1232g(j)(1)(A) (authorizing Attorney General to compel production of educational records "relevant to an authorized investigation" related to terrorism); 38 U.S.C. § 4326(a) (providing that Secretary of Veterans Affairs shall have "the right to copy and receive . . . any documents of any person or employer that the Secretary considers relevant to the investigation"). Indeed, in at least one respect the language of Section 215 is more restrictive: While other such statutes authorize the government to compel the production of records in "investigations" or "authorized investigations," Section 215 is unique in further limiting the kinds of "authorized investigation[s]" that can permissibly serve as predicates for disclosure orders. *See* 50 U.S.C. § 1861(b)(2)(A) (providing that disclosure orders may not be predicated on authorized investigations that are merely "threat assessment[s]").[6]

Section 215's relevance requirement is also significantly narrower than that used by courts in the grand-jury context. *Compare id.* § 1861(b)(2) ("reasonable grounds to believe that the tangible things sought *are relevant* to an authorized investigation" (emphasis added)), *with United States v. R. Enters., Inc.*, 498 U.S. 292, 293 (1991) ("no reasonable possibility that the category of materials the Government seeks *will produce information relevant to the general subject* of the grand jury's investigation").[7]

---

[6] *Compare* Dep't of Justice, Attorney General's Guidelines for Domestic FBI Operations 17–20 (2008), http://1.usa.gov/ebNZw7 (distinguishing factually predicated investigations from "threat assessments"), *with In re Special Feb. 1975 Grand Jury*, 565 F.2d 407, 411 (7th Cir. 1977) ("A grand jury necessarily holds broad powers of inquiry into any conduct possibly violating federal criminal laws . . . . A grand jury may properly investigate on the basis of tips, rumors, hearsay, speculation or any other source of information . . . ." (citation omitted)).

[7] Notably, the government's theory gives no significance at all to Congress's decision, in 2006, to impose a *higher* standard for the acquisition of records under 50 U.S.C. § 1861 ("relevant to an authorized investigation"), in place of the lower standard originally written into

If Congress had intended to afford the government the extraordinary authority to obtain records "necessary to the application of investigative techniques," Gov't Br. 24, it would surely have said so in clearer language. *See Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001) (Congress "does not, one might say, hide elephants in mouseholes."); *Lynch v. Alworth-Stephens Co.*, 267 U.S. 364, 370 (1925) ("[T]he plain, obvious and rational meaning of a statute is always to be preferred to any curious, narrow, hidden sense that nothing but the exigency of a hard case and the ingenuity and study of an acute and powerful intellect would discover." (quotation marks omitted)). Congress would not have used the same language used in run-of-the-mill administrative subpoena statutes. It would not have expressly limited the scope of Section 215 orders to the kinds of information obtainable under grand-jury subpoenas and similar instruments. And it would not have limited the kinds of investigations that can serve as predicates for such orders. The government's theory of the statute is irreconcilable with the statute's plain text.

Unsurprisingly, courts that have applied the "related to an authorized investigation" standard in other contexts have refused to give it anything approaching the scope the government gives it here. For example, in *In re Sealed Case*, 42 F.3d 1412 (D.C. Cir. 1994), the D.C. Circuit considered the lawfulness of an administrative subpoena issued in connection with an investigation into a particular bank. The subpoena sought personal financial records from the bank's directors to determine whether they had derived financial benefits from the use of certain accounts, whether they had the capacity to pay civil penalties, and whether they had engaged in "other wrongdoing, as yet unknown." *Id.* at 1419. Citing *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950), the court wrote that the subpoena would be proper insofar as it sought

---

the Patriot Act ("sought for an authorized investigation"). *Compare* Pub. L. 109-177, § 106(b), 120 Stat. 192, 196 (2006), *with* Pub. L. 107-56, § 215, 115 Stat. 272, 287–88 (2001).

information "relevant to the investigation—the boundary of which may be defined quite generally." *In re Sealed Case*, 42 F.3d at 1419 (emphasis omitted). Applying that permissive standard, the court nonetheless invalidated the subpoena's demand for records relating to "other wrongdoing, as yet unknown." Administrative subpoena power, the court wrote, "does not afford [the government] unfettered authority to cast about for potential wrongdoing." *Id*. at 1418.

The government's theory of the statute also lacks any meaningful limiting principle. The government reassures the Court that telephony metadata is "fundamentally distinguish[able]" from other kinds of records because call records "interconnect with one another." Gov't Br. 28–29. But many other kinds of records interconnect with one another. If all U.S. residents' call records are relevant, why would their location information not be relevant as well? Surely it would be useful to the government to have a comprehensive database of citizens' comings and goings—who was meeting with whom, and when, and where. The same is true of financial records. Terrorists and other criminals are notorious, after all, for their ability to transfer funds through multiple accounts in order to conceal the funds' origin and destination. Surely, a comprehensive database of financial transactions would allow the government to "help identify clandestine terrorist operatives or networks within the United States." Gov't Br. 29.[8]

The government's defense of the program ultimately boils down to an argument that the Court should read Section 215 sweepingly because the statute provides a tool useful in national security investigations. Such investigations, the government argues, "often have remarkable breadth, spanning long periods of time and multiple geographic regions." Gov't Br. 25. But

[8] In fact, the NSA is reportedly exploiting many types of records (including location and financial information) precisely because they *do* reveal such associational interconnections. James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. Times, Sept. 28, 2013, http://nyti.ms/1fxW2c6.

national security investigations are not unique in this regard.[9] More fundamentally, the government's argument is not about what the statute actually says but about what it would like the statute to say. That is an argument that should be directed to Congress, not this Court.

2. The government's construction of Section 215 is impossible to reconcile with the larger statutory scheme.

Beyond its incompatibility with the statute's plain text, the government's theory of Section 215 is irreconcilable with the larger statutory scheme. At the very same time that Congress enacted Section 215 in 2001, *see* Pub. L. 107-56, § 215, 115 Stat. 272, 287, it added a separate provision to the Stored Communications Act ("SCA") that specifically *prohibits* the disclosure of call records by telephone companies to the government, *see id.* § 212(a)(1)(B)(iii), 115 Stat. at 284 (codified at 18 U.S.C. § 2702(a)(3)). Congress provided specific exceptions to that general prohibition, but Section 215 is not among them. *See id.* §§ 2702(a)(3), 2702(c), 2703(c). Moreover, 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'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)(1) (authorizing installation and use of "pen register" and "trap and trace" device); *id.* § 1842(d) (stating that order granting approval to install or use such a device must include, among other things, the identities of the persons to be investigated and

[9] *See, e.g.*, *United States v. Hayes*, No. 12-MAG-3229 (S.D.N.Y. Dec. 12, 2012) (criminal complaint alleging conspiracy and fraudulent manipulation of the London Interbank Offered Rate set by global financial-services companies based in the United States, United Kingdom, Germany, Switzerland, and Japan).

monitored). To adopt the government's theory would require the Court to conclude that a general provision—Section 215—permits what more specific provisions disallow. *See In re Stoltz*, 315 F.3d 80, 93 (2d Cir. 2002) ("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))).

Notably, concerns about an analogous end run have led many courts to prohibit the government from using the SCA, 18 U.S.C. § 2701 *et seq.*, 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, 2009 WL 8231744, at *3, *8 (E.D. Ky. Apr. 17, 2009); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005). The government contends that "[c]ourts including this one" have held that the government may obtain orders requiring prospective record production under the SCA. Gov't Br. 30. But this view has been adopted by only a small minority of judges, whose approach has been specifically rejected by a number of courts—indeed, "including this one." *See, e.g.*, *In re Application of U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel.*, 2009 WL 159187, at *3–*4 (S.D.N.Y. Jan. 13, 2009); *United States v. Espudo*, No. 12-CR-236, 2013 WL 3803912, at *8 (S.D. Cal. July 19, 2013).

The government's theory is inconsistent with the larger statutory scheme in another respect as well. Like other subsections of FISA, Section 215 entrusts the FISC, not the executive, with the task of determining whether the statute's substantive standards have been met. FISA's subsections are structured in this way because Congress concluded that particularized judicial oversight was necessary to safeguard constitutional rights. *See, e.g.*, S. Rep. No. 95-604, pt.1, at

8 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904. 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. In this way, however, the government's theory of Section 215 reassigns to the executive a task that Congress assigned to the FISC.

3. The government's argument that Congress "ratified" its construction of Section 215 is incorrect.

The government contends that Congress ratified the mass call-tracking program when it reauthorized Section 215 in 2010 and 2011. *See* Gov't Br. 27. The doctrine of congressional ratification, however, operates only when Congress is "well aware of, and legislate[s] on the basis of" judicial or administrative interpretations of its laws. *Atkins v. Parker*, 472 U.S. 115, 140 (1985). That is emphatically not the case here.

First, the government cannot satisfy the basic predicate of the doctrine of legislative ratification—that Congress was aware of the FISC's secret interpretation of Section 215. *See, e.g.*, *Apex Hosiery Co. v. Leader*, 310 U.S. 469, 488–89 (1940) (crediting ratification where "the application of the statute . . . ha[d] been fully brought to the attention of the public and the Congress"). Some members of Congress have said they were never informed of that interpretation, *see, e.g.*, Sensenbrenner Amicus Br. 7–10, and the government points to no evidence contradicting those claims. Instead, the government implies that Congress had *constructive* knowledge of the FISC's interpretation because the government provided "*all* members of Congress . . . access" to information about the program. Gov't Br. 27. That contention is doctrinally inadequate. *See Comm'r of Internal Revenue v. Glenshaw Glass Co.*, 348 U.S. 426, 431 (1955) ("Re-enactment—particularly without the slightest affirmative indication that Congress ever had the [relevant] decision before it—is an unreliable indicium at

best."). It is also factually incorrect. Many members of the House of Representatives elected in 2010 were never allowed access to the administration's briefing paper on Section 215 before voting to reenact the Patriot Act in 2011. *See* Peter Wallsten, *House Panel Withheld Document on NSA Surveillance Program from Members*, Wash. Post, Aug. 16, 2013, http://wapo.st/1cTBZmh. Those members were forced to rely, instead, on the executive's public descriptions of the NSA's surveillance authorities, some of which were "clearly erroneous." *See, e.g.*, Letter from James Clapper, Dir. of Nat'l Intelligence, to Sen. Dianne Feinstein (Jun. 21, 2013), http://1.usa.gov/1fEcW6w.

Second, even those members of Congress who knew of the FISC's secret interpretation of Section 215 were not permitted to debate it publicly. *See, e.g.*, Letter from Sen. Ron Wyden & Sen. Mark Udall to Eric Holder, Att'y Gen. (Sept. 21, 2011), http://1.usa.gov/190sAls. The doctrine of legislative ratification has never been applied in such extraordinary circumstances. *See, e.g.*, *United States v. Calamaro*, 354 U.S. 351, 359 (1957) (deeming reenactment to be "without significance" where it was "not accompanied by any congressional discussion which throws light on [the] intended scope" of the relevant interpretation).

Finally, Congress cannot be presumed to have ratified an interpretation of Section 215 that contradicts its plain meaning. *See Biddle v. Comm'r of Internal Revenue*, 302 U.S. 573, 582 (1938) ("Where the law is plain the subsequent re-enactment of a statute does not constitute adoption of its administrative construction.").

B. Plaintiffs' statutory claim is not impliedly precluded.

Plaintiffs bring their statutory challenge to the mass call-tracking program in reliance on the express and unambiguous waiver of sovereign immunity in the Administrative Procedure Act ("APA"), 5 U.S.C. § 702. The waiver contained in the APA reflects a "strong presumption that

Congress intends judicial review of administrative action." *Bowen v. Mich. Acad. of Family Physicians*, 476 U.S. 667, 670 (1986); *see also Natural Res. Def. Council v. Johnson*, 461 F.3d 164, 172 (2d Cir. 2006). This presumption is the backdrop against which Congress has legislated since 1976, when it amended the APA to provide an avenue for precisely the type of non-monetary relief that Plaintiffs seek here. *See* Pub. L. 94-574, 90 Stat. 2721 (1976). Nonetheless, the government argues that two different statutes impliedly overcome that presumption here: 18 U.S.C. § 2712 and Section 215 itself, 50 U.S.C. § 1861. Neither section expresses, by word or by implication, the exception the government urges on the Court.

1. There is a strong presumption in favor of judicial review under the APA.

Section 702 of the APA permits a "person suffering legal wrong because of agency action" to bring suit against the United States and its officers for "relief other than money damages." 5 U.S.C. § 702. Congress provided this waiver of sovereign immunity "to provide broadly for judicial review of [agency] actions, affecting as they do the lives and liberties of the American people." *Cohen v. United States*, 650 F.3d 717, 723 (D.C. Cir. 2011) (quoting *Natural Res. Def. Council v. Hodel*, 865 F.2d 288, 318 (D.C. Cir. 1988)). This waiver of sovereign immunity does not apply, however, "if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702(2); *see also id*. § 701(a)(1).

Because of the "strong presumption" in favor of judicial review under the APA, *Bowen*, 476 U.S. at 670, this exception is "construed narrowly." *Johnson*, 461 F.3d at 171. The presumption may only be overcome "upon a showing of "clear and convincing evidence of a contrary legislative intent [to] restrict access to judicial review." *Bowen*, 476 U.S. at 671 (quotation marks omitted). That evidence may be found in the statute's "express language, but also [in] the structure of the statutory scheme, its objectives, its legislative history, and the nature

of the administrative action involved." *Johnson*, 461 F.3d at 171 (quoting *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 345 (1984)). Congressional intent to preclude judicial review must be "fairly discernible" from the statutory scheme. *Id*. at 172 (quoting *Block*, 467 U.S. at 351). Ambiguity, if any, is resolved in favor of the APA's waiver: "[W]here substantial doubt about the congressional intent exists, the general presumption favoring judicial review of administrative action is controlling." *Id.*

In arguing that any ambiguity runs in its favor, the government confuses Plaintiffs' APA claim, which relies on an express waiver of sovereign immunity, with other types of claims that do not have the benefit of the APA's blanket presumption. The difference is an important one. Claims for money damages are not covered by the APA's general waiver of sovereign immunity; in the absence of that presumption, courts must find a separate waiver and, in doing so, they apply a narrow view. *See, e.g.*, *FAA v. Cooper*, 132 S. Ct. 1441, 1446, 1448 (2012) (interpreting narrowly the Privacy Act's waiver of sovereign immunity for "actual damages"). But where a plaintiff seeks non-monetary relief pursuant to the APA's waiver, as here, the standard is reversed: courts construe *exceptions* to the APA's waiver of sovereign immunity narrowly. *Johnson*, 461 F.3d at 171; *see also Bowen*, 476 U.S. at 670.

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

For an implied exception to the APA's waiver of sovereign immunity, the government looks first to 18 U.S.C. § 2712. This section provides a cause of action against the United States for damages based upon willful violations of the SCA, the Wiretap Act, and three specific subsections of FISA: 106(a), 305(a), and 405(a) (codified at 50 U.S.C. §§ 1806(a), 1825(a), and 1845(a)). The government speculates that this damages provision implicitly forecloses certain claims arising not just under the three discrete subchapters of FISA in which those subsections

appear (relating to traditional wiretapping, physical searches, and pen registers and trap-and-trace devices), Gov't Br. 17, but those arising under *other* provisions of FISA, including Section 215. But no speculation is required; Congress spelled out precisely the preclusive effect of section 2712:

> **Exclusive Remedy.—** Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims *within the purview of this section*.

18 U.S.C. § 2712(d) (emphasis added). As described above, subsection (a) makes clear exactly which claims fall under this section's preclusive umbrella, and claims under Section 215 are not among them. *See id.* § 2712(a). Notably, whereas Congress named the Wiretap Act and the SCA in their entirety, it named only three specific subsections within FISA. *See id.*[10]

The government also argues that Congress's failure to add a new damages clause to section 2712 when it amended Section 215 in 2006 shows that Congress did not intend violations of Section 215 to have any remedy at all. Gov't Br. 17 & n.6 (discussing 50 U.S.C. § 1861(h)). But this is an extraordinary and unsupported leap. In 2006, Congress amended Section 215 to add a "use" provision similar to that contained in 50 U.S.C. §§ 1806(a), 1825(a), and 1845(a). *See* 50 U.S.C. § 1861(h). Legislators could have adjusted the remedy provided in section 2712 to

[10] The government's reliance on *Jewel v. NSA*, No. C 08-04373, 2013 WL 3829405 (N.D. Cal. July 23, 2013), is misplaced. *See* Gov't Br. 17–18. To the extent that the government reads *Jewel* to eliminate injunctive relief under FISA altogether, that result contradicts the plain terms of the exclusive-remedy provision in subsection 2712(d) and ignores Congress's deliberate effort to distinguish its wholesale treatment of the Wiretap Act and the SCA from its selective treatment of FISA. *Jewel* held at most that section 2712 precluded certain claims arising under one of the three specific subchapters of FISA that section 2712 identifies. *See* 2013 WL 3829405, at *10–12.

Moreover, the FISA provisions identified in section 2712 pertain only to the use and disclosure of information under FISA, not to its initial collection. Plaintiffs are "bringing a different claim, seeking different relief." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2209 (2012).

include Section 215's new "use" provision. But Congress chose not to do so and, despite the government's assertions, gave no indication that this choice carried any preclusive effect.

As often occurs when it seeks to avoid the APA's broad waiver of sovereign immunity, the government "reads too much into congressional silence." *Michigan v. U.S. Army Corps of Eng'rs*, 667 F.3d 765, 775 (7th Cir. 2011). In particular, no matter what Congress did, the government would imply an intent to foreclose review here: whether Congress had spoken by amending section 2712 to account for its addition of 50 U.S.C. § 1861(h) in 2006, or remained silent as it did, the government would draw the same conclusion. That cannot be right. It would replace the APA's strong presumption in favor of judicial review with a logic that forecloses judicial review at every turn.

3. Plaintiffs' statutory claim is not precluded by Section 215 itself.

The government's secondary theory for preclusion fares no better. The government argues that the provision allowing recipients to challenge Section 215 orders, added in 2006, manifests a congressional intent to bar all other claims and relief under this section. *See* Gov't Br. 18–19; 50 U.S.C. § 1861(f). But, again, this argument goes too far, turning Congress's attempt to clarify the availability of one species of review into a silent subtraction of every other type of remedy. There is no evidence of such intent. As the Supreme Court observed last year, "if the express provision of judicial review in one section of a long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it would not be much of a presumption at all." *Sackett v. EPA*, 132 S. Ct. 1367, 1373 (2012).

The government argues that the addition of 50 U.S.C. § 1861(f) in 2006 was a deliberate effort to "limit[] the right to contest the legality of Section 215 production orders" to recipients, Gov't Br. 18, but the legislative history shows that Congress added 50 U.S.C. § 1861(f) merely

to "clarify" an already-existing remedy. In doing so, Congress gave no indication that it intended to displace other existing remedies, including those provided by the APA. *See* H.R. Rep. 109-174, pt. 1, at 6, 77, 106 (repeatedly describing the addition of this subsection as an effort to "clarify" the statute). Indeed, at the time, the government concurred in the view that this addition did not represent a significant change in the law. *See, e.g.*, *Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary*, 109th Cong. at 106 (2005) ("Patriot Act HJC Hearing") (testimony of Kenneth Wainstein, U.S. Attorney for the District of Columbia).

The purpose of this change was a familiar and unsurprising one: Congress simply made explicit recipients' ability to go before a judge to challenge a production order, as is customary with ordinary subpoenas. *See, e.g.*, Fed. R. Crim. P. 17(c); Patriot Act HJC Hearing at 65 (statement of Robert Khuzami) (amendment designed to "place Section 215 proceedings on a par with grand jury proceedings"). It did so, in part, because the legal process available to recipients of records demands under a similar statute, 18 U.S.C. § 2709 (national security letters), had been the subject of litigation. *See, e.g.*, *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 507 (S.D.N.Y. 2004); Patriot Act HJC Hearing at 105-06, 140-42 (discussing *Doe*). But in the course of clarifying the procedures for raising such an objection under Section 215, Congress nowhere altered—or even considered—the APA's background presumption, especially as it applies to the subjects of record requests.

As a matter of statutory structure, nothing in the recipient-review procedure bars the traditional APA review that Plaintiffs seek here—rather, they are complimentary remedies. Recipients may challenge a Section 215 production order but, as with subpoenas, this does not inevitably imply an intent to bar the *subject* of a records request from bringing her own

challenge. Contrary to the government's assertion, courts in this district routinely allow third parties to contest subpoenas on grounds other than privilege—including their asserted privacy interests. *Compare* Gov't Br. 19 n.8, *with Arias-Zeballos v. Tan*, No. 06 Civ. 1268, 2007 WL 210112, *1 (S.D.N.Y. Jan. 25, 2007) (listing cases).

Relying on *Block*, 467 U.S. at 349, the government argues that because Section 215 provides for recipient challenges, it impliedly precludes judicial review "at the behest of other persons," like Plaintiffs. *See* Gov't Br. 18–19. But as courts have recognized, this assumption is too simplistic. In particular, the D.C. Circuit has cautioned against reading *Block* "too broadly," especially where the interests of the various parties may diverge or the statute bears directly on the class to which the plaintiff belongs. *Ark. Dairy Co-op Ass'n, Inc. v. U.S. Dep't of Agr.*, 573 F.3d 815, 822–23 (D.C. Cir. 2009). Tellingly, the court did so in a case involving the very same statute that the Supreme Court interpreted in *Block*, finding that the APA afforded a right of review to milk *producers* despite the fact that the statutory scheme at issue granted such a right only to milk *handlers*. *Id.*at 823; *see Koretoff v. Vilsack*, 614 F.3d 532, 536–40 (D.C. Cir. 2010); *Council for Urological Interests v. Sebelius*, 668 F.3d 704, 710 (D.C. Cir. 2011) (distinguishing *Block* where agency action had "direct" and "substantial" impact on plaintiffs); *see also Pottawatomi*, 132 S. Ct. at 2209 (rejecting comparison to *Block*). Even in *Block* itself, the Supreme Court evaluated the availability of judicial review under the APA by taking into account a proxy's willingness to pursue a plaintiff's interests. 467 U.S. at 352.

Without question, these concerns apply to Section 215. Indeed, "no recipient of any Section 215 Order has challenged the legality of such an Order." *See* 2013 FISC Opinion at 15–16. That is perhaps because recipients are shielded from liability for complying with such orders, *see* 50 U.S.C. § 1861(e), and thus their interests diverge from those of the orders' subjects. *See*

Strengthening Privacy Rights and National Security: Hearing Before the S. Comm. on the Judiciary, 113th Cong. at 4 (2013), http://bit.ly/19CVPgl (statement of Marc Zwillinger, Yahoo! counsel) (describing "institutional pressures and procedural disincentives against levying a [provider] challenge" to a FISC order).

The cases discussed above demonstrate that a statute's silence with respect to one class of plaintiffs or claims does not invariably imply that those plaintiffs have no road to court. The government's "effort to transform silence into implicit prohibition would seriously undermine Congress's effort in the APA to authorize specific relief against the United States." *U.S. Army Corps of Eng'rs*, 667 F.3d at 775. It takes more to show "clear and convincing evidence" of Congress's intent to strip the APA's remedies and preclude review. For instance, in *Dew v. United States*, 192 F.3d 366, 371–74 (2d Cir. 1999), the Second Circuit carefully analyzed the comprehensiveness of the statutory scheme at issue, the express signs of intent in the legislative history, and the parallel structure of a similar statute—ultimately concluding that each of these factors favored preclusion. In this case, one can hardly say the same.

If there were any doubt, Congress has shown in a related context—the SCA—that it knows how to create a comprehensive and exclusive remedial scheme when it wants to. In *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114 (E.D. Va. 2011), the court considered the carefully drawn remedies that the SCA makes available to internet-service subscribers. *See id.* 127–28. It found that the statute barred a Twitter subscriber's pre-execution challenge to certain disclosure orders, pointing to the SCA's plain statement that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for non-constitutional violations of this chapter." *Id.* at 129 (quoting 18 U.S.C. § 2708). If Congress had intended to preclude claims under Section 215, it did not need to look far to find

the right words. Yet the government would render provisions like this all but superfluous by imputing the very same intent to Congress even in their absence.

III. Plaintiffs have stated a claim under the Fourth Amendment.

Plaintiffs' Complaint states a claim that 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, therefore, constitutes a search. This search violates the Fourth Amendment because it is warrantless and because it lacks any of the usual indicia of reasonableness.

A. 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*, 533 U.S. at 33. 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. *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.").

As an initial matter, Plaintiffs have a subjective expectation of privacy in their telephony metadata. Plaintiffs ACLU and NYCLU work on a wide range of civil-liberties and human-rights issues, including issues relating to national security, access to reproductive services, racial discrimination, the rights of immigrants, and discrimination based on sexual orientation and

gender identity. Compl. ¶¶ 24, 26. In connection with this work, ACLU and NYCLU staff frequently talk by telephone with individuals relating to potential legal representation in suits against the federal government. *Id.* ¶ 25. Often, the mere fact that Plaintiffs have communicated with these individuals is sensitive. *Id.* Plaintiffs similarly communicate with potential witnesses, informants, or sources—including, in particular, government and industry whistleblowers—who regard the fact of their association or affiliation with Plaintiffs as confidential. *Id.* ¶¶ 26–27.

Moreover, the expectation that telephony metadata will not be subjected to long-term recording and aggregation by the government is objectively reasonable. The kind of surveillance at issue here hands the government a comprehensive record of Americans' associations, revealing a wealth of detail about their familial, political, professional, religious, and intimate relationships—the same kind of information that could traditionally only be obtained by examining the contents of communications. *Id.* ¶¶ 1, 35. For example, certain telephone numbers are used for a single purpose, and their use can reveal a person's religion, 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. Aggregating metadata across time can yield an even richer repository of personal and associational details.

This surveillance 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 955–56 (Sotomayor, J., concurring) ("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. . . ."); *id*. at 955 (Individuals have "a reasonable societal expectation of privacy in the sum of [their] public movements.").

What Justice Sotomayor observed of long-term location tracking is equally true of the mass call-tracking program. Indeed, the program is in several respects considerably more intrusive than the location tracking that was at issue in *Jones*. That 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.

The government's motion to dismiss Plaintiffs' Fourth Amendment claim relies heavily on *Smith v. Maryland*, 442 U.S. 735 (1979), but nothing in *Smith* remotely suggests that the Constitution permits the indefinite collection of sensitive information about every single phone call made or received by residents of the United States. In *Smith*, the Supreme Court upheld the installation of a "pen register" in a criminal investigation. Gov't Br. 31–33. 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. 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*.

The government contends, again citing *Smith*, that individuals lack a constitutionally protected privacy interest in telephony metadata because that information has been shared with telephone companies. Gov't Br. 32–33. But the government's reading of *Smith* fails to account for *Jones* and a host of Supreme Court cases recognizing that in sharing information with the public or a third party, individuals do not necessarily surrender their expectation of privacy. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *id*. at 964 (Alito, J., concurring); *see also, e.g.*, *Florida v. Jardines*, 133 S. Ct. 1409 (2013) (odors detectable by a police dog that emanate outside of a home); *Kyllo*, 533 U.S. 27 (thermal signatures emanating from a home); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (diagnostic-test results held by hospital staff). These cases confirm that an individual's expectation of privacy in information does not hinge simply on whether she has shared it with another person. Were it otherwise, even the *contents* of one's phone calls or email would be constitutionally unprotected, as both are shared with third parties.

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.

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

1. 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 a general warrant for the digital age. *See Berger v. New York*, 388 U.S. 41, 59 (1967).

The government's motion implies that the warrant requirement does not apply in this case because the mass call-tracking programs serves "special government needs." Gov't Br. 35. But the "special needs" doctrine applies "[o]nly in those exceptional circumstances," *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring), in which the primary purpose of the government's actions is above and beyond criminal law enforcement, *Ferguson v. City of Charleston*, 532 U.S. 67, 81–86 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41–47 (2000), and special needs "make the warrant and probable-cause requirement impracticable," *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (quoting *T.L.O.*, 469 U.S. at 351).

The application of the warrant and individualized-suspicion requirements would not compromise the government's asserted interest in targeting specific, known phone numbers to determine who is in contact with suspected terrorists.[11] Congress itself has recognized that the Fourth Amendment's core requirements of individualized suspicion and prior judicial approval are not impracticable in the gathering of foreign intelligence. *See, e.g.*, 50 U.S.C. § 1804 (electronic surveillance); 50 U.S.C. § 1824 (physical searches). It has applied that same judgment even when legislating authority for the collection of information identical to that collected under the mass call-tracking program. *See* 50 U.S.C. § 1842 (installation of pen register or a trap-and-trace device to gather telephony metadata). It may be true that the government can acquire the limited subset of phone records it will eventually seek more rapidly by maintaining a database of the records of every phone call made in the country. But the Supreme Court has never dispensed with the Fourth Amendment's core constraints based on simple expedience. *See, e.g.*, *Carroll v. United States*, 267 U.S. 132, 153–54 (1925); *United States v. Barbera*, 514 F.2d

[11] *See, e.g.*, Press Release, Sen. Ron Wyden & Sen. Mark Udall, Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs (June 19, 2013), http://1.usa.gov/17pMDzH ("In fact, we have yet to see any evidence that the bulk phone records collection program has provided any otherwise unobtainable intelligence.").

294, 301–02 (2d Cir. 1975). Moreover, in any true emergency the government could satisfy the exigent-circumstances exception to the warrant requirement. *See Missouri v. McNeely*, 133 S. Ct. 1552, 1570 (2013).[12]

For these reasons, the special-needs doctrine does not apply in this case. Even if it did, the government would still bear the burden of establishing that the manner in which it pursues its interests is reasonable. *See Illinois v. Lidster*, 540 U.S. 419, 426 (2004). For the reasons below, it is not.

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

Even if the warrant and probable-cause requirements do 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. *See 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." 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).

[12] The special-needs doctrine does not apply for the additional reason that the government's primary purpose in the mass call-tracking program is often indistinguishable from—not "above and beyond"—the needs of law enforcement. *See, e.g.*, 50 U.S.C. § 1801(e) (defining "foreign intelligence" to include information relating to crimes such as "international terrorism"); *United States v. Abu-Jihaad*, 630 F.3d 102, 127 (2d Cir. 2010) ("[M]ultiple purposes may be inevitable given FISA's definition of 'foreign intelligence information' . . . .").

"[T]he ultimate touchstone of the Fourth Amendment" is "reasonableness," *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the "totality of circumstances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008). In the context of electronic surveillance, reasonableness demands that statutes 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).

The principal question in conducting the Fourth Amendment's balancing inquiry is 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. The intrusion in this case upon Plaintiffs' privacy is substantial: The government has acquired and continues to acquire a record of every single call made to or by Plaintiffs; as explained above, those records contain a wealth of revealing information that can be every bit as sensitive as the actual contents of Plaintiffs' calls. In fact, the mass call-tracking program lacks any of the indicia of reasonableness to which the Supreme Court has traditionally looked. *See, e.g.*, *Berger*, 388 U.S. at 55–56, 59–60 (invalidating surveillance statute due to the breadth, lack of particularity, and indefinite duration of the surveillance it authorized); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 300, 320 (1972) (invalidating warrantless wiretap authorized by the Attorney General "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government").

First, the program authorizes surveillance that is suspicionless. Under the mass call-tracking program, the government acquires the telephone records of virtually every American. This weighs heavily against the program's reasonableness. *See 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.").

Second, the mass call-tracking program allows surveillance that is essentially indefinite. 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); *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 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 *information* that is relevant to an investigation and information that is not. The program's lack of particularity is yet another factor that weighs heavily against its reasonableness. *See 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 interests. The government's stated interest is in "identifying and tracking terrorist operatives."

Gov't Br. 36. To achieve this goal, the government could simply collect the phone records of those about whom it has at least some quantum of suspicion. The government need not collect everyone's call records in order to discover information about a discrete number of individuals. *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 192 (2d Cir. 2004) (To satisfy reasonableness, "the means employed must bear 'a close and substantial relation' to the government's interest in pursuing the search." (citation omitted) (quoting *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 676 (1989))).

Contrary to the government's claim, Gov't Br. 36, the limits on the government's later use of Plaintiffs' sensitive information do not mitigate the mass call-tracking program's privacy intrusion. The search, for Fourth Amendment purposes, occurs when the government acquires Plaintiffs' telephony metadata. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("[A] violation of the [Fourth] Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion." (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974))); *accord Soldal v. Cook Cnty.*, 506 U.S. 56, 67, n.11 (1992). If that were not so, the government could constitutionally record every phone call made and copy every email sent by every American every single day, so long as, for example, it only searched the resulting database upon probable cause and judicial authorization.

The cases relied upon by the government—to argue that limitations on the use of information can reduce the invasiveness of a search—do not help its cause. *See* Gov't Br. 36. Critical to the Supreme Court's analysis in each of those cases was a factor not present here: the diminished expectation of privacy of the class of persons searched. *See Maryland v. King*, 133 S. Ct. 1958, 1978 (2013) (comparing the "reduced" expectation of privacy of one arrested on probable cause for a dangerous offense with that of "the average citizen"); *Vernonia Sch. Dist.*

47J v. Acton, 515 U.S. 646, 665 (1995) (diminished expectation of privacy of student athletes "[t]he most significant element in this case"); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 830–32 (2002) (same). Moreover, the invasiveness of the collection of Plaintiffs' phone records far exceeds those at issue in the government's cases. In *King*, for example, the State of Maryland took DNA samples from certain arrestees for the sole purpose of creating DNA fingerprints that revealed nothing more than the individuals' identities. 133 S. Ct. at 1979 ("[T]he CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee."). In this case, however, the government collects and stores Plaintiffs' telephony metadata for the very purpose of later querying it.

IV. Plaintiffs have stated a claim under the First Amendment.

Separate from their Fourth Amendment claim, Plaintiffs allege that the mass call-tracking program violates their First Amendment rights to private association and free speech. Compl. ¶¶ 3, 37. Courts have repeatedly recognized that the government's investigatory and surveillance activities can infringe on rights protected by the First Amendment—and that the First Amendment has force independent of the Fourth Amendment. *See, e.g.*, *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963); *Tabbaa v. Chertoff*, 509 F.3d 89, 102–03 & n.4 (2d Cir. 2007); *LaRouche*, 817 F.2d at 234–35; *Local 1814*, 667 F.2d at 269. In particular, courts apply "exacting scrutiny" when investigatory tools 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 requires the government to show that the program is the least restrictive means of pursuing a compelling state interest. *See Clark*, 750 F.2d at 95.

The government's mass call-tracking program burdens First Amendment rights by exposing all of Plaintiffs' associational contacts to government monitoring and scrutiny. Compl. ¶¶ 3, 35. As explained above, Plaintiffs routinely engage in sensitive or confidential communications by phone with their members, donors, current and potential clients, whistleblowers, legislators and their staffs, other advocacy organizations, and members of the public. *Id.* ¶¶ 3, 24–27. In its breadth and scope, the NSA's bulk metadata collection far exceeds the demands for basic membership rolls that produced *NAACP v. Alabama*, 357 U.S. 449 (1958), and its progeny, *see Bates v. City of Little Rock*, 361 U.S. 516 (1960); *Gibson*, 372 U.S. 539.

A corollary of this direct intrusion on Plaintiffs' associational privacy is the chill it imposes on their work. Compl. ¶¶ 24–27, 35. Generalized surveillance on this scale "chills associational and expressive freedoms." *See Jones*, 132, S. Ct. at 956 (Sotomayor, J., concurring). This harm amounts to a substantial and discrete burden on Plaintiffs' First Amendment rights.

A. The First Amendment's protection is distinct from and often greater than that afforded by the Fourth Amendment.

The First Amendment's protections do not vanish simply because, as the government argues, investigative activities also implicate the Fourth Amendment. *See* Gov't Br. 38. The interests guarded by these rights are distinct. *See Tabbaa*, 509 F.3d at 102–03 n.4; *Ealy v. Littlejohn*, 569 F.2d 219, 227 (5th Cir. 1978) ("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."). The First Amendment's protection is often greater than that afforded by the Fourth Amendment alone. 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 v. Texas*, 379 U.S. 476, 485 (1965)); *see Marcus v. Search Warrant*, 367 U.S. 717 (1961).

The Second Circuit has recognized that the Fourth Amendment does not serve as a substitute for First Amendment interests, because the rights are not coextensive. In *Tabbaa*, the court considered the border search of five U.S. citizens returning from a religious conference in Toronto. After concluding that the searches and detentions did not violate the Fourth Amendment, the Second Circuit conducted a separate First Amendment analysis:

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

509 F.3d at 102 n.4.[13]

[13] The government relies extensively on Judge Wilkey's opinion in *Reporters Committee for Freedom of the Press v. AT&T Co.*, 593 F. 2d 1030 (1978), as both the roadmap and chief authority for its attacks on Plaintiffs' First Amendment claim. *See* Gov't Br. 38–40. What it does not acknowledge, however, is that the D.C. Circuit was deeply fractured in its holding, with Judge Wilkey unable to command a majority for any of the First Amendment views on which the government relies. *See Reporters Comm.*, 593 F. 2d at 1071 n.4 (Robinson, J., concurring in part) (refusing to join portion of the opinion addressing the relationship between the plaintiffs' First and Fourth Amendment claims and stating that "the analysis appropriate for First Amendment issues concentrates on the burden inflicted on protected activities, and the result may not always coincide with that attained by application of Fourth Amendment doctrine"); *id.* at 1079–97 (Wright, J., dissenting).

The government also fails to acknowledge that Judge Wilkey's analysis was superseded only a few years later in *Clark v. Library of Congress*, 750 F.2d 89 (D.C. Cir. 1984). There, a unanimous panel of the D.C. Circuit held that First Amendment protections applied to an FBI full-field investigation of the plaintiff. Analyzing the Supreme Court's First Amendment holdings, it explained that "[s]ignificant impairments" of the First Amendment "right to form political beliefs and lawful associations without governmental intrusion or compelled disclosure" "must withstand exacting scrutiny and may not be justified on a showing of a mere legitimate state interest." *Id*. at 94.

In some cases, safeguards required by the Fourth Amendment may in practice satisfy the First Amendment as well. *See, e.g.*, *Zurcher*, 436 U.S. at 565; *United States v. Ramsey*, 431 U.S. 606, 623–24 (1977). But that does not mean that the First Amendment has no application at all to investigative activities.[14] A criminal search warrant, carefully drawn and supported by probable cause, 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. *See Gibson*, 372 U.S. at 546; *Local 1814*, 667 F.2d at 269; *LaRouche*, 817 F.2d at 234–35; *Paton v. La Prade*, 469 F. Supp. 773 (D.N.J. 1978).

The government's position is even more extreme than it lets on, for it argues that Plaintiffs' First Amendment interests "are safeguarded by adherence to Fourth Amendment standards" at the same time it contends that the Fourth Amendment does not bear on Plaintiffs' claims at all. *Compare* Gov't Br. 37–38, *with* Gov't Br. 31–35. This position would, in effect, banish the First Amendment even in cases where *no* Fourth Amendment safeguards apply. That cannot be right, and the government's cases do not stand for that proposition.

Here, even if the Court were to conclude that the third-party records doctrine extinguishes Plaintiffs' Fourth Amendment interest in their telephony metadata, Plaintiffs' independent First Amendment claim would still stand. The expressive and associational interests protected by the First Amendment are not controlled by the third-party records doctrine. *See N.Y. Times Co. v. Gonzales*, 459 F.3d 160, 167–68 (2d Cir. 2006) (finding reporters' First Amendment interests

[14] To support its argument, the government relies on two out-of-circuit cases, *Gordon v. Warden Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983), and *United States v. Mayer*, 503 F.3d 740, 747–48 (9th Cir. 2007), but in both cases the court reached the merits of the plaintiff's First Amendment claim.

implicated by subpoena to third-party provider for phone records); *Local 1814*, 667 F.2d at 269 (similar for union payroll records).

B. Both direct and indirect burdens on First Amendment rights must withstand exacting scrutiny.

The government argues that Plaintiffs' First Amendment claim fails because the mass call-tracking program is not "specifically directed" at Plaintiffs' associational activities, Gov't Br. 39—but the intrusion could not be more direct. The program's very purpose is to collect and analyze records of Plaintiffs' telephonic associations, as well as those of millions of other Americans. *See* Gov't Br. 24 ("The bulk collection of telephony metadata is necessary to enable discovery of otherwise hidden connections between individuals"); *id*. at 6 (describing contact-chaining analysis). The NSA collects this metadata precisely because it provides a direct and detailed map of who is associating with whom.

But even if the substantial burden on Plaintiffs' First Amendment rights is characterized as indirect, the standard is the same: the program must satisfy exacting scrutiny. It does not matter whether the restraint on First Amendment freedoms is deliberate or, as the government would have it, the byproduct of some other initiative. The Supreme Court has repeatedly emphasized that a First Amendment injury does not depend on an intent to curtail speech. *See, e.g.*, *Bates*, 361 U.S. at 523 ("Freedoms such as these are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference."). Where the burden on Plaintiffs' rights is substantial, exacting scrutiny applies. Indeed, "[t]his 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)).

The government's discussion seeks to blur the line between an "incidental" burden—that is, one that is unintended—and a *de minimis* one. *See* Gov't Br. 39 (quoting *Reporters Comm.*, 593 F.2d at 1052). But they are two very different things. The Constitution does not bar the government from conducting a good-faith criminal investigation that has only a fleeting or minor impact on First Amendment rights. Nor does it bar a more intrusive investigation that is the least-restrictive means of pursuing a compelling governmental interest. But the government may not employ "unduly broad means having an unnecessary impact on protected rights of speech, press, or association" to achieve even "justifiable governmental goals." *In re Grand Jury Proceedings*, 776 F.2d at 1103 (quotation marks omitted). This is precisely the failing of the government's indiscriminate collection of all Americans' call records: it is broad beyond all limits, and carries with it an unreasonable and unnecessary invasion of Plaintiffs' First Amendment rights.

As many have observed since the disclosure of the mass call-tracking program, the breadth of the program is unprecedented. No other law-enforcement demand has involved the disclosure of Americans' telephone communications on such wholesale terms. As a direct result, the program's intrusion on associational privacy and its chilling effect on protected expression are on a scale without ready comparison. In these qualities, the program puts a wholly new calculus before the Court—one which fails the exacting-scrutiny standard, and cannot be saved by even the purest motives.

CONCLUSION

For the foregoing reasons, this Court should deny Defendants' Motion to Dismiss.

Dated: October 1, 2013

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)
Patrick Toomey (PT-1452)
Brett Max Kaufman (BK-2827)
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