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.

13 Civ. 3994 (WHP)

ECF Case

DEFENDANTS' MEMORANDUM OF LAW
IN SUPPORT OF MOTION TO DISMISS THE COMPLAINT

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney
U.S. Department of Justice
Washington, D.C.

PREET BHARARA
United States Attorney for
the Southern District of New York

DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
Tel. No. (212) 637-2739 (Jones)
Fax No. (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

TABLE OF CONTENTS

Page

PRELIMINARY STATEMENT..... 1

STATEMENT OF FACTS..... 2

A. Statutory Background..... 2

B. The Collection of Telephony Metadata Records Authorized by the FISC..... 4

C. Plaintiffs' Allegations..... 7

ARGUMENT..... 9

POINT I: THE COMPLAINT SHOULD BE DISMISSED BECAUSE PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING..... 9

A. The Requirements of Article III Standing..... 9

B. Plaintiffs Allege Injuries That Are Speculative and Conjectural, Not Certainly Impending..... 11

POINT II: CONGRESS IMPLIEDLY PRECLUDED JUDICIAL REVIEW OF PLAINTIFFS' STATUTORY CLAIM..... 14

POINT III: THE GOVERNMENT'S BULK COLLECTION OF TELEPHONY METADATA IS AUTHORIZED UNDER SECTION 215..... 19

A. The Telephony Metadata Collected Under the FISC's Orders Are "Relevant" to Authorized National Security Investigations..... 20

1. Congress Intended Section 215 To Incorporate a Broad Concept of Relevance, Drawn from the Legal Meaning Applied in Grand Jury, Civil, and Administrative Proceedings, That Also Takes Into Account the Special Characteristics of the Terrorism Investigations to Which It Applies..... 21

2. Congress Has Legislatively Ratified the Construction of Section 215 as Allowing for the Bulk Collection of Telephony Metadata Records..... 26

3. Telephony Metadata Are "Relevant" Within the Meaning of Section 215 Because Bulk Collection of the Data Enhances the Government's Ability To Detect Terrorist Operatives and Prevent Terrorist Attacks…… 28

B. Nothing in the Text of Section 215 Prohibits the Collection of Records "as They Are Generated"…….. 29

POINT IV: THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA DOES NOT VIOLATE PLAINTIFFS' FOURTH AMENDMENT RIGHTS …….. 31

A. Plaintiffs Have No Fourth Amendment Privacy Interest in Telephony Metadata…….. 31

B. The Government's Acquisition of Metadata Is Reasonable…… 35

POINT V: PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA VIOLATES THE FIRST AMENDMENT …….. 37

A. Plaintiffs' Failure To Allege An Actionable Fourth Amendment Claim Is Also Fatal To Their First Amendment Claim 37

B. Plaintiffs Make No Allegations That the Government's Collection of Telephony Metadata Is Intended to Curtail Protected Expressive or Associational Activity…… 39

CONCLUSION…….. 40

TABLE OF AUTHORITIES

Cases ***Page(s)***

ACLU Found. of S. California v. Barr,
952 F.2d 457 (D.C. Cir. 1991) 38

Am. Civil Liberties Union v. Nat'l Sec. Agency,
493 F.3d 644 (6th Cir. 2007) 38

Ashcroft v. Iqbal,,
556U.S. 662 (2009) ..... *passim*

Atkins v. Parker,
472 U.S. 115 (1985) 28

Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls,
536 U.S. 822 (2002) 36

Block v. Cmty. Nutrition Inst., 467 U.S. 340 (1984) 16, 19

Block v. N. Dakota ex rel. Bd. of Univ. & Sch. Lands,
461 U.S. 273 (1983) 16

C.I.A. v. Sims,
471 U.S. 159 (1985) 25

Carrillo Huettel, LLP v. U.S. S.E.C.,
2011 WL 601369 (S.D. Cal. Feb. 11, 2011) 22

Chambers v. Time Warner, Inc.,
282 F.3d 147 (2d Cir. 2002) 5, 6

Clapper v. Amnesty Int'l USA,
133 S. Ct. 1138 (2013) ..... *passim*

Conopco, Inc. v. Roll Int'l,
231 F.3d 82 (2d Cir. 2000) 5

DaimlerChrysler Corp. v. Cuno,
547 U.S. 332 (2006) 9, 10

Dew v. United States,
192 F.3d 366 (2d Cir. 1999) 19

E.E.O.C. v. Shell Oil Co.,
466 U.S. 54 (1984) 21, 28

F.A.A. v. Cooper,
132 S. Ct. 1441 (2012) 15

F.T.C. v. Invention Submission Corp.,
965 F.2d 1086 (D.C. Cir. 1992) 22

FDIC v. Meyer,
510 U.S. 471 (1994) 15

Forest Grove Sch. Dist. v. T.A.,
557 U.S. 230 (2009) 28

Gordon v. Warren Consol. Bd. of Educ.,
706 F.2d 778 (6th Cir. 1983) 38

Goshawk Dedicated Ltd. v. Am. Viatical Servs., LLC,
2007 WL 3492762 (N.D. Ga. Nov. 5, 2007) 22

Guest v. Leis,
255 F.3d 325 (6th Cir. 2001) 33

Haig v. Agee,
453 U.S. 280 (1981) 28, 36

In re Adelphia Commc'ns Corp.,
338 B.R. 546 (Bankr. S.D.N.Y. 2005) 22

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) 19, 33

In re Application of the United States,
632 F. Supp. 2d 202 (E.D.N.Y. 2008) 30

In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448 (S.D.N.Y. 2006) 30

In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act,
551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008) 36

In re Grand Jury Proceedings,
616 F.3d 1186 (10th Cir. 2010) 21

In re Grand Jury Proceedings: Subpoenas Duces Tecum,
827 F.2d 301 (8th Cir. 1987) 22, 35

In re Motion for Release of Court Records,
526 F. Supp. 2d 484 (Foreign Intel. Surv. Ct. 2007) 3

In re Subpoena Duces Tecum,
228 F.3d 341 (4th Cir. 2000) 22

Jabara v. Kelley,
476 F. Supp. 561 (E.D. Mich. 1979)..... 38

Jewel v. Nat'l Sec. Agency,
2013 WL 3829405 (N.D. Cal. July 23, 2013).....17

Katz v. United States,
389 U.S. 347 (1967)..... 32

Kiobel v. Royal Dutch Petroleum Co.,
621 F.3d 111(2d Cir. 2010)..... 7

Laird v. Tatum,
408 U.S. 1 (1972)..... 14, 39

Langford v. Chrysler Motors Corp.,
513 F.2d 1121 (2d Cir. 1975)..... 19

Lorillard v. Pons,
434 U.S. 575 (U.S. 1978)..... 28

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992)..... 10, 14

Maryland v. King,
133 S. Ct. 1958 (2013)..... 35, 36

Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak,
132 S. Ct. 2199 (2012)..... 15-16

McLean v. United States,
566 F.3d 391 (4th Cir. 2009) 23

Medtronic Sofamor Danek, Inc. v. Michelson,
229 F.R.D. 550 (W.D. Tenn. 2003) 22

Members of City Council of City of Los Angeles v. Taxpayers for Vincent,
466 U.S. 789 (1984)..... 39

Michigan Dep't of State Police v. Sitz,
496 U.S. 444 (1990)..... 36, 37

Minnesota v. Carter,
525 U.S. 83 (1998) 35

N.L.R.B. v. Am. Med. Response, Inc.,
438 F.3d 188 (2d Cir. 2006)..... 21, 23

N.L.R.B. v. Amax Coal Co.,
453 U.S. 322 (1981).....22

Oklahoma Press Pub. Co. v. Walling,
327 U.S. 186 (1946)..... 25, 29

Oneida Indian Nation of New York v. State of N.Y.,
691 F.2d 1070 (2d Cir. 1982)..... 27

Oppenheimer Fund, Inc. v. Sanders,
437 U.S. 340 (1978).....21

PBGC. ex rel. St. Vincent Catholic Med. Centers Ret. Plan v. Morgan Stanley Inv. Mgmt. Inc., 712 F.3d 705 (2d Cir. 2013)..... 9

Port Washington Teachers' Ass'n v. Bd. of Educ. of Port Washington Union free Sch. Dist.,
478 F.3d 494 (2d Cir. 2007)..... 14

Quon v. Arch Wireless Operating Co., Inc.,
529 F.3d 892 (9th Cir. 2008) 33

Rakas v. Illinois,
439 U.S. 128 (1978)..... 35

Redd v. City of Enter.,
140 F.3d 1378 (11th Cir. 1998) 38

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.,
593 F.2d 1030 (D.C. Cir. 1978)..... 38, 39, 40

S.E.C. v. Jerry T. O'Brien, Inc.,
467 U.S. 735 (1984)..... 34

Smith v. Bowersox,
159 F.3d 345 (8th Cir. 1998) 23

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

Socialist Workers Party v. Attorney Gen. of U.S.,
510 F.2d 253 (2d Cir. 1974)..... 39

Steagald v. United States,
451 U.S. 204 (1981)..... 35

Steel Co. v. Citizens for a Better Env't,
523 U.S. 83 (1998) 10

United States v. Aguilar,
883 F.2d 662 (9th Cir. 1989) 39

United States v. Anderson-Bagshaw,
2012 WL 774964 (N.D. Ohio Mar. 8, 2012) 34

United States v. Forrester,
512 F.3d 500 (9th Cir. 2008) 33

United States v. Gering,
716 F.2d 615 (9th Cir. 1983) 38

United States v. Hill,
459 F.3d 966 (9th Cir. 2006) 22

United States v. Jones,
132 S. Ct. 945 (2012) 32, 34

United States v. Kennedy,
81 F. Supp. 2d 1103 (D. Kan. 2000) 33

United States v. Martinez-Fuerte,
428 U.S. 543 (1976) 36, 37

United States v. Mayer,
503 F.3d 740 (9th Cir. 2007) 38

United States v. Maynard,
615 F.3d 544 (D.C. Cir. 2010) 34

United States v. Merrick Sponsor Corp.,
421 F.2d 1076 (2d Cir. 1970) 5

United States. v. Miller,
425 U.S. 435 (1976) 18-19, 33, 34

United States v. Mitchell,
445 U.S. 535 (1980) 15

United States v. R. Enterprises, Inc.,
498 U.S. 292 (1991) 21, 23

United States v. Ramsey,
431 U.S. 606 (1977) 38

United States v. Rigmaiden,
2013 WL 1932800 (D. Ariz. May 8, 2013) 35

United States v. Shabani,
513 U.S. 10 (1994) 23

United States v. Smith,
426 F.3d 567 (2d Cir. 2005) 36

United States v. Upham,
168 F.3d 532 (1st Cir. 1999) 22

Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.,
454 U.S. 464 (1982) 9

Vernonia Sch. Dist. 47J v. Acton,
515 U.S. 646 (1995) 35, 36

Whitmore v. Arkansas,
495 U.S. 149 (1990) 10

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 38, 39

STATUTES

5 U.S.C. § 701 ..... 15, 18

5 U.S.C. § 702 ..... 8, 15

18 U.S.C. § 2703 30

18 U.S.C. § 2712 16,17

50 U.S.C. § 1801 18

50 U.S.C. § 1803 ..... 3, 4

50 U.S.C. § 1806 ..... 17, 18

50 U.S.C. § 1821 18

50 U.S.C. § 1825 ..... 17, 18

50 U.S.C. § 1841 18

50 U.S.C. § 1845 ..... 17, 18

50 U.S.C. § 1861 ..... *passim*

50 U.S.C. § 1862 ..... 7, 26

50 U.S.C. § 1871 ..... 7, 27

50 U.S.C.. § 1881a 12

RULES AND REGULATIONS

47 C.F.R. § 42.6 30

FEDERAL RULES OF CIVIL PROCEDURE

Fed. R. Civ. P. 12(b)(6) 7

Fed. R. Civ. P. 26(b)(1) 24

FEDERAL RULES OF CRIMINAL PROCEDURE

Fed. R. Crim. P. 41(e)(2)(B) 22

LEGISLATIVE MATERIAL

S. 2369, 109th Cong., 2d Sess. (2006) 24

S. Rep. No. 109-85 (2005) 26

S. Rep. No. 111-92 (2009) 28

S. Rep. No. 112-13 (2011) 28

H.R. Rep. No. 94-1656 (1976) 16

H.R. Rep. 109-174 (2005) 18, 23, 25, 26

151 Cong. Rec. S13636 (Dec. 15, 2005) 23

151 Cong. Rec. S14275-01 (2005) 24

152 Cong. Rec. H581-02 (2006) 24

152 Cong. Rec. S1325 (Feb. 15, 2006) 25

152 Cong. Rec. S1379 (Feb. 16, 2006) 23

152 Cong. Rec. S1598-03 (2006) 23, 24

156 Cong. Rec. H838 (Feb. 25, 2010) 27

156 Cong. Rec. S2109 (Mar. 25, 2010) 27

OTHER AUTHORITIES

D. Kris & J. Wilson, *National Security Investigations & Prosecutions* (2d ed. 2012) …… 4, 17

PRELIMINARY STATEMENT

Plaintiffs seek to invalidate an important element of the Government's efforts to protect the Nation from the very real and unrelenting threat of terrorist attack. Specifically, Plaintiffs challenge the Government's bulk collection of "telephony metadata," business records created by (and belonging to) telecommunications service providers that include such information as the time and duration of calls made, and the numbers dialed, but not the content of anyone's calls, or their names and addresses. Collection of these records, which has been repeatedly authorized by the Foreign Intelligence Surveillance Court (FISC) as consistent with governing law, permits National Security Agency (NSA) analysts, acting under strict controls imposed by FISC orders, to detect communications between foreign terrorists and any of their contacts located in the United States. Plaintiffs maintain that this activity is unauthorized by the Foreign Intelligence Surveillance Act (FISA), and violates the First and Fourth Amendments. For the reasons discussed herein, the Court lacks jurisdiction to entertain these claims, and Plaintiffs fail in any event to state claims on which relief can be granted. Thus, the Complaint should be dismissed.

First, Plaintiffs' Complaint fails to establish their standing to sue, as their alleged injuries are entirely speculative. The FISC's orders limit review of the metadata for intelligence purposes to those records responsive to queries conducted using identifiers (*e.g.*, telephone numbers) chosen based on reasonable, articulable suspicion that they are associated with foreign terrorist organizations approved for targeting by the FISC. There is no non-speculative basis to expect that queries of the metadata under this standard will return information about calls either made by Plaintiffs, or made to them by others. Thus, Plaintiffs' allegations that records of their calls could be used to glean sensitive information about their work and clients, and that persons with whom they collaborate could be "chilled" by that prospect from contacting them, are wholly conjectural. Second, Congress impliedly precluded review of Plaintiffs' statutory claim, that the

bulk collection of telephony metadata exceeds the Government's authority under FISA. FISA's detailed statutory scheme for judicial review of specified intelligence activities conducted under its purview reflects a Congressional purpose to preclude third parties such as Plaintiffs from mounting FISA-based challenges to FISC business records orders in federal district court.

Apart from these jurisdictional deficiencies, the Government's collection of telephony metadata is lawful under FISA and the Constitution, and the Complaint states no plausible claim to the contrary. As the FISC repeatedly has found (as recently as last month), telephony metadata are relevant to authorized counter-terrorism investigations, and their collection by the Government is authorized by FISA. Plaintiffs also fail to state a Fourth Amendment claim. There has been no search or seizure of their property or effects, and, as the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), telephone subscribers have no protected privacy interest in the type of information at issue here. In addition, even if the Government's conduct implicated a protected Fourth Amendment interest, the bulk collection of telephony metadata would be "reasonable" and permissible in light of the strong national interest in preventing terrorist attacks, and the minimal intrusion on individual privacy. Finally, Plaintiffs fail to state a First Amendment claim, because intelligence-gathering conducted in a manner consistent with the Fourth Amendment, for purposes unrelated to the suppression of protected speech or association, does not violate the First Amendment. For these reasons, elaborated below, the Court should reject Plaintiffs' effort to preclude the use of this important intelligence tool.

STATEMENT OF FACTS

A. Statutory Background

Congress enacted FISA to authorize and regulate certain governmental surveillance of communications and other activities conducted for purposes of gathering foreign intelligence. In enacting FISA, Congress also created the FISC, an Article III court of 11 appointed U.S. district

judges with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of intelligence-gathering by the Government. 50 U.S.C. § 1803(a); *see In re Motion for Release of Court Records,* 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

At issue here is the "business records" provision of FISA, 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("Section 215"). Section 215 authorizes the FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism" (provided, in the case of a counter-terrorism investigation of a "United States person," that "such investigation … is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"). 50 U.S.C. § 1861(a)(1). The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things. *Id.* § 1861(c)(2)(D).

The Government's application for an order under Section 215 must include, among other things, a statement of facts showing that there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation … to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism." *Id.* § 1861(b)(2)(A). The investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor thereto). *Id.* § 1861(a)(2)(A), (b)(2)(A). Information acquired from the records or other tangible items received in response to a Section 215 order "concerning any United States person may be used and disclosed by [the Government] without the consent of [that] person only in accordance with … minimization procedures," adopted by the Attorney General and enumerated in the Government's application, that "minimize the retention, and prohibit the dissemination, of

nonpublicly available information concerning unconsenting United States persons consistent with the [Government's] need … to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1861(b)(2)(B), (g)(2), (h). The FISC must find that these requirements have been met before it issues the requested order, which in turn must direct that the minimization procedures described in the application be followed. *Id.* § 1861(c)(1).

Section 215 includes a scheme providing for judicial review of a business records order, but only in limited circumstances. Specifically, it allows "[a] person receiving a production order [to] challenge the legality of that order" by filing a petition with the "review pool" of FISC judges designated under 50 U.S.C. § 1803(e)(1) to review production orders under Section 215. *Id.* § 1861(f)(1), (2)(A)(i). A "pool" judge considering a petition to modify or set aside a production order may grant the petition if the judge finds that the order does not meet the requirements of Section 215 or "is otherwise unlawful." *Id*. § 1861(f)(2)(B). Thus, a production order can be set aside if it exceeds the authority conferred by Section 215 or is unconstitutional. 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions § 19:10 at 714 (2d ed. 2012) ("Kris & Wilson"). Either the Government or a recipient of a production order may appeal the decision of the pool judge to the FISC Court of Review, with review available thereafter on writ of certiorari in the Supreme Court. 50 U.S.C. § 1861(f)(3); *see id.* § 1803(b). Section 215's carefully circumscribed provisions for judicial review were added when Congress reauthorized the USA PATRIOT Act in 2006, and these provisions authorized contested litigation before the FISC for the first time. 1 Kris & Wilson §5:5, 19:7 (2d ed. 2012). The FISA does not provide for review of Section 215 orders at the behest of third parties.

B. The Collection of Telephony Metadata Records Authorized by the FISC

Plaintiffs challenge the Government's exercise of authority, as reflected in a secondary order of the FISC, to collect telephony metadata records in bulk. Compl. ¶ 30, citing *In re*

Application of the FBI for an Order Requiring the Production of Tangible Things [etc.], Dkt. No. BR 13-80, Secondary Order 1-2 (F.I.S.C. Apr. 25, 2013) (the "Secondary Order") (Exhibit 1, hereto). The Secondary Order was issued in conjunction with, and on the same day as, a primary order in which the FISC granted the Government's application for production of these records, finding "reasonable grounds to believe that the [records] sought are relevant to authorized investigations … being conducted by the FBI … to protect against terrorism." *In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR 13-80, Primary Order 1-2 (F.I.S.C. Apr. 25, 2013) (the "Primary Order") (Exhibit 2, hereto). [1]

These Orders directed the daily production to NSA of electronic copies of "all call detail records, or 'telephony metadata,'" created by a recipient telecommunications service provider for calls to, from, or wholly within the United States. Primary Order at 3-4; Secondary Order at 1-2. "Telephony metadata" is defined by the Orders as "comprehensive communications routing information" including but not limited to "originating and terminating telephone number[s], International Mobile Subscriber Identity (IMSI) number[s], International Mobile Station Equipment Identity (IMEI) number[s], trunk identifier[s], telephone calling card numbers, and time and duration of call." Primary Order at 3 n.1. By the express terms of the Orders, "[t]elephony metadata does not include the name, address, or financial information of a subscriber or customer." *Id.*; Secondary Order at 2. The Court's Orders do not permit the Government to listen to or record the contents of any telephone conversations.

As required by FISA, the terms of the Primary Order direct the Government to comply with "minimization procedures" that strictly limit the extent to which information received under

[1] The Court may consider the Secondary Order on this motion, as it is specifically referenced in and integral to the Complaint. *See Chambers v. Time Warner, Inc.*, 282 F.3d 147, 152 (2d Cir. 2002). The Court may take judicial notice of the publicly available portions of the Primary Order as an official judicial act. *See Conopco, Inc. v. Roll Int'l,* 231 F.3d 82, 86 n.3 (2d Cir. 2000); *United States v. Merrick Sponsor Corp.,* 421 F.2d 1076, 1079 n.2 (2d Cir. 1970).

the FISC's Orders can be reviewed, used, or disseminated, and prevent Government personnel from indiscriminately sifting through the data. *See* 50 U.S.C § 1861(b)(2)(B), (g)-(h); Primary Order at 4-14. The metadata must be stored by NSA in secure networks with access restricted to authorized personnel who have received appropriate training. Primary Order at 4-5. NSA analysts may "query" (electronically search) the metadata "for purposes of obtaining foreign intelligence information" – that is, to identify terrorism-related communications – only when there is reasonable, articulable suspicion, based on specific facts, that the "identifier" (*e.g.*, a telephone number) used to query the database is associated with a specific foreign terrorist organization that was previously identified to and approved for targeting by the FISC. Primary Order at 6-8; DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013) ("DNI Statement") (Exhibit 3, hereto) at 2.[2] Only a small number of NSA officials designated by the Primary Order are authorized to make findings of reasonable, articulable suspicion, and NSA's Office of General Counsel (OGC) must review such findings for numbers reasonably believed to be used by United States persons, to ensure the findings are not based on activities protected by the First Amendment. Primary Order at 7-9. Although the FISC has authorized the collection and maintenance of large amounts of metadata, only those records responsive to queries based on approved identifiers may be disseminated. *See id.* at 12-13. Therefore, "only a small fraction of the records are ever reviewed." DNI Statement at 2.

The results of these "contact-chaining queries," Primary Order at 6, following analysis by NSA, may be shared with the FBI and allow Government investigators to discover persons, including persons (and associates of persons) located in the United States, who have been in contact with known or suspected terrorist organizations and may themselves be engaged in

[2] The Court may consider this statement on the Government's motion to dismiss because it is a document "of which [P]laintiffs had possession and relied on in bringing suit." *Chambers,* 282 F.3d at 152 (internal quotation marks and citation omitted)*; see* Compl. ¶ 31.

terrorist activity. DNI Statement at 1-2; *see* Primary Order at 4. However, before the NSA may disseminate information about a U.S. person outside the agency, a high-ranking NSA official "must determine that the information identifying the U.S. person is in fact related to counterterrorism information and is necessary to understand the counterterrorism information or assess its importance." Primary Order at 13. The FBI, in turn, must handle the information it receives from NSA in accordance with the minimization procedures set forth in *The Attorney General's Guidelines for Domestic Operations. Id.* at 4.

The NSA's activities under the FISC's Orders are subject, in addition, to an extensive regime of internal reporting, audits, and oversight; regular consultation with the NSA Office of the Inspector General, and the Department of Justice, to assess compliance with the FISC's Orders; and monthly reports to the FISC including, *inter alia*, a discussion of NSA's application of the "reasonable, articulable suspicion" standard and the number of times that query results containing U.S. person information have been shared with anyone outside NSA. *Id.* at 4-16. As acknowledged in the Complaint, ¶ 31, the FISC must renew Government's authority to collect telephony metadata under its orders every 90 days. *See* Primary Order at 17 (setting expiration date of collection authority); Secondary Order at 4 (same).[3]

C. Plaintiffs' Allegations[4]

Plaintiffs are non-profit organizations that engage in civil rights litigation, education, and lobbying. Compl. ¶¶ 6-9, 24. They allege that the Government has engaged in "dragnet

---

[3] FISA also requires the Government to report to Congress regarding the use of its Section 215 authority, including copies of significant FISC orders and the Government's supporting pleadings. 50 U.S.C. §§ 1862, 1871.

[4] For purposes of a motion to dismiss under Fed. R. Civ. P. 12(b)(6), the well-pleaded factual allegations of a complaint must be accepted as true. *Kiobel v. Royal Dutch Petroleum Co.*, 621 F.3d 111, 124 (2d Cir. 2010). Defendants reserve the right, however, to contest Plaintiffs' allegations, and/or their ability to prove their allegations without implicating protected state secrets, as may be necessary or appropriate in further proceedings.

acquisition" of telephony metadata concerning their communications, *id.* ¶¶ 1-2, 30, although they acknowledge that the collection of the metadata is court-authorized. *Id.* ¶¶ 2, 22, 23, 31.

Plaintiffs contend that the telephony metadata provide the government with "a comprehensive record" of "sensitive and often privileged" information about their communications with "journalists, current and potential clients, legislators and legislative staff, and members of the public," concerning "Plaintiffs' advocacy, representation of clients, and efforts to lobby Congress." Compl. ¶¶ 3, 24-25, 35. These include communications with potential witnesses and informants, whistleblowers, and lobbyists who consider their associations with Plaintiffs confidential. *Id.* ¶¶ 26-27. Plaintiffs specifically allege that the telephony metadata maintained by the Government "could readily be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations, as well as those whom Plaintiffs contact in connection with their work." Id. ¶¶ 1, 35. Therefore, the Government's maintenance of these records, according to Plaintiffs, "is likely to have a chilling effect on whistleblowers and others who would otherwise contact Plaintiffs." Id. ¶¶ 3, 35. Plaintiffs make no allegations, however, that the Government has reviewed metadata of any of their communications, whether pursuant to queries based on reasonable, articulable suspicion that particular telephone numbers (or other identifiers) are associated with specific foreign terrorist organizations approved for targeting by the FISC, or otherwise.

Plaintiffs contend that this court-sanctioned collection of telephony metadata exceeds the authority conferred by Section 215, and violates the First and Fourth Amendments. *Id.* ¶¶ 36-38. They bring suit under the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202, predicating jurisdiction on, *inter alia*, the waiver of sovereign immunity codified in the Administrative Procedure Act, 5 U.S.C. § 702. *Id.* ¶ 4. Plaintiffs seek a declaration that the telephony metadata collection is unlawful; a permanent injunction against future collection of telephony metadata

concerning their communications, whether under the Secondary Order "or any successor thereto"; and an order directing the Government "to purge from [its] possession" all such metadata collected to date. *Id.* at 10 (Prayer for Relief ¶¶ 2-5).

ARGUMENT

Under the pleading standards set forth in *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), to survive a motion to dismiss a complaint must contain "sufficient factual matter, accepted as true, to state a claim that is plausible on its face." Mere "labels and conclusions," and "naked assertion[s] devoid of further factual enhancement," are not sufficient. Rather, considering only the well-pleaded, non-conclusory allegations of a complaint, and "assum[ing] their veracity," the court must determine whether they "plausibly give rise to an entitlement to relief." *Id.* at 678-79 (internal quotations omitted), *see id.* at 680-81; *PBGC ex rel. St. Vincent Catholic Med. Ctr. Ret. Plan v. Morgan Stanley Inv. Mgmt., Inc.*, 712 F.3d 705, 717 (2d Cir. 2013) ("*St. Vincent").* To reach the level of plausibility, the well-pleaded facts "must demonstrate 'more than a sheer possibility that a defendant has acted unlawfully.'" *St. Vincent*, 712 F.3d at 717 (quoting *Iqbal*, 556 U.S. at 678). Facts that "are merely consistent with" a defendant's liability "stop[ ] short of the line between possibility and plausibility." *Iqbal,* 556 U.S. at 678; *St. Vincent,* 712 F.3d at 717. The Complaint in this case falls well short of that line, and must be dismissed.

POINT I: THE COMPLAINT SHOULD BE DISMISSED BECAUSE PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING

A. The Requirements of Article III Standing

"The judicial power of the United States" is limited by Article III of the Constitution "to the resolution of 'cases' and 'controversies.'" *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.,* 454 U.S. 464, 471 (1982). "No principle is more fundamental to the judiciary's proper role in our system of government." *DaimlerChrysler Corp. v. Cuno,* 547 U.S. 332, 341 (2006) (internal quotation marks and citation omitted). A

demonstration by plaintiffs of their standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992), "serv[ing] to prevent the judicial process from being used to usurp the powers of the political branches." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013) (citations omitted). The "standing inquiry has been especially rigorous when reaching the merits of the dispute would force [a court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Id.* at 1147 (citations and quotations omitted). Similarly, as the Supreme Court recently observed in *Amnesty Int'l,* it has "often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs." *Id.*

To establish Article III standing, Plaintiffs must seek relief from an injury that is "'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Id.* Although "imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending." *Id.* (citations and internal quotation marks omitted); *see also id.* ("'threatened injury must be *certainly impending* to constitute injury in fact,'" and "'[a]llegations of *possible* future injury' are not sufficient" (quoting *Whitmore v. Arkansas,* 495 U.S. 149, 158 (1990), and citing multiple additional cases)); *see also DaimlerChrysler,* 547 U.S. at 345. If Plaintiffs cannot carry the threshold jurisdictional burden of adequately pleading their standing to sue, *see Defenders of Wildlife,* 504 U.S. at 561, then "the [C]ourt cannot proceed" and must dismiss the case. *Steel Co. v. Citizens for a Better Env't,* 523 U.S. 83, 94 (1998).

B. Plaintiffs Allege Injuries That Are Speculative and Conjectural, Not Certainly Impending

The Complaint should be dismissed because Plaintiffs have failed to plausibly allege an injury meeting Article III's standards. As discussed below, Plaintiffs' allegations of the consequences they will suffer as a result of the challenged intelligence-gathering activities depend on speculation that the Government has reviewed, or might in future review, call detail records of their communications, and that persons who would otherwise contact Plaintiffs by telephone may be "chilled" from doing so by that conjectural prospect. Such speculation is insufficient for purposes of Article III, and, as a result, Plaintiffs lack standing.

Plaintiffs' allegations of injury stem from their assertion that for purposes of civil rights litigation, education, and lobbying they engage in "sensitive" and "privileged" communications with clients, witnesses, whistleblowers, and other persons who consider their associations and "even the fact of their discussions" with Plaintiffs to be confidential. Compl. ¶¶ 3, 6-9, 24-27. They allege that metadata records of their calls "could readily be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations, as well as those whom Plaintiffs contact in connection with their work." *Id.* ¶ 35. On the basis that records of their calls "could readily be used" for this purpose, Plaintiffs allege further that the Government's acquisition of such records "is likely to have a chilling effect on people who would otherwise contact Plaintiffs." *Id.* These allegations are too conjectural to demonstrate that "the threatened injur[ies] [are] certainly impending." *Amnesty Int'l,* 133 S. Ct. at 1147.

Plaintiffs' first alleged harm, the potential use of call detail records to identify persons with whom Plaintiffs speak, cannot support their standing. Government personnel could identify persons with whom Plaintiffs speak by phone, either individually or collectively, only by retrieving and reviewing the metadata records of calls to or from Plaintiffs (and then taking the next step of ascertaining the identities of the subscribers whose numbers are memorialized in the

records). But under the FISC's Orders, Government personnel may only review records responsive to queries initiated using identifiers that are believed, based on reasonable, articulable suspicion, to be associated with specific foreign terrorist organizations approved for targeting by the FISC. *See supra* at 6; Primary Order at 7. The Complaint contains no allegations, much less well-pleaded, non-conclusory allegations, that the Government has accessed or reviewed metadata records of Plaintiffs' calls as a result of queries made under the "reasonable, articulable suspicion" standard (or otherwise). Thus, it is sheer speculation to suggest that metadata records of calls to or from Plaintiffs either have been or ever will be retrieved or reviewed through queries of the database, much less mined by the Government "to learn sensitive and privilege information about [Plaintiffs'] work and clients." Compl. ¶ 3.[5]

The Supreme Court's decision in *Amnesty Int'l* addressed a similar standing question and establishes that Plaintiffs' reliance on speculation concerning the reach of Government intelligence-gathering activities is insufficient to demonstrate their standing. In *Amnesty Int'l*, various humans rights, labor, and media organizations challenged the constitutionality of the FISA Amendments Act of 2008, which expanded the Government's authority to intercept the communications of non-U.S. persons located abroad. 133 S. Ct. at 1144. The organizations alleged that they interacted and engaged in sensitive communications with persons who were likely to be considered by the Government as potential terrorists, or persons of interest in

[5] In a 2011 FISC opinion recently declassified and publicly released by the Government (concerning the adequacy of the Government's minimization procedures for Internet communications data collected under authority of section 702 of FISA, 50 U.S.C. § 1881a), the FISC alluded to a 2009 opinion in which it found that, due to "misperceptions by the FISC" and "inaccurate statements made in the government's submissions," the "NSA had been routinely running queries of [telephony] metadata [collected under Section 215] using query terms that did not meet the required standard." October 3, 2011, FISC Memorandum Opinion and Order (Bates, J.) at 16 n.14 (available at http://icontherecord.tumblr.com/tagged/declassified). Any allegation by Plaintiffs, however, that past incidents of non-compliance with the "reasonable, articulable suspicion" standard make it likely that records of their calls have been or will be reviewed, would be equally speculative, and insufficient under Article III.

terrorism investigations. *See id.* at 1145-46. They further alleged that they would suffer harms as a result of the Government surveillance program, including a compromised ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information," and a need to undertake various costly measures to avoid possible surveillance. *Id.*

The Supreme Court, however, held that none of these alleged harms was sufficient to confer standing, because it was "speculative whether the Government will imminently target communications to which respondents are parties." *Id.* at 1148. Rather, the Court held that the plaintiffs' harm rested on a "speculative chain of possibilities," including "that the Government [would] target the communications of non-U.S. persons with whom they communicate," that the Government would succeed in intercepting those communications, and that the plaintiffs would be parties to the particular communications the Government intercepts. *Id.* at 1148-50. So, too, here. The idea that the course of unspecified Government counter-terrorism investigations would lead to particular telephone numbers; that these numbers would be reasonably suspected of association with unidentified foreign terrorist organizations; that these numbers would be used to formulate queries of the collected telephony metadata; and that these queries would retrieve metadata records of Plaintiffs' calls that the Government would in turn review, is just as speculative as the allegations of harm that were rejected as insufficient in *Amnesty Int'l.*

Equally unavailing as a claim of injury is the asserted possibility that others might refrain from communicating with Plaintiffs because they fear disclosure of their associations with Plaintiffs. Plaintiffs allege that, because the metadata records of their calls "could readily be used to identify" those with whom Plaintiffs communicate, individuals who would otherwise contact Plaintiffs will "likely" be chilled from doing so. Compl. ¶ 35. Plaintiffs' burden, however, is to allege facts plausibly suggesting that their injury is certainly impending. *Iqbal,* 556 U.S. at 678; *Amnesty Int'l.* 133 S. Ct. at 1147. The "naked assertion," *Iqbal,* 556 U.S. at

678, that unnamed individuals who regard their communications with Plaintiffs as "confidential" may be so unnerved by the idea of the Government reviewing telephony metadata that they will refrain from calling Plaintiffs does not suffice. The Complaint is "devoid of further factual enhancement" that elevates this allegation from the field of mere possibility to the required crest of plausibility. *Id.* That is especially so because the occurrence of the alleged injury "depends on the unfettered choices made by independent actors not before the court[ ] … whose exercise of broad and legitimate discretion the court[ ] cannot presume . . . to predict." *Defenders of Wildlife,* 504 U.S. at 562. In this event, it becomes the Plaintiffs' burden "to adduce facts showing that those choices have been or *will be* made in such manner" as to produce cognizable harm, *id.* (emphasis added), which the Complaint does not even endeavor to do. *See also Port Washington Teachers' Ass'n v. Bd. of Educ*., 478 F.3d 494, 499 (2d Cir. 2007) (teachers' union lacked standing to challenge policy on reporting student pregnancies where they failed to show that "students will bring suit against [them] for [making] any such disclosure[s]").

In addition, even if as yet unnamed third persons refrained from contacting Plaintiffs out of fear that their association with Plaintiffs could be revealed, that would not constitute an injury attributable to the Government's actions. Rather, such a decision by third parties would instead be the product of subjective and speculative fears on the part of those individuals that the Government might retrieve and review metadata records of their calls with Plaintiffs. As such it would not be "fairly traceable" to the Government's exercise of authority under Section 215. *Amnesty Int'l,* 133 S. Ct. at 1152 & n.7, citing *Laird v. Tatum,* 408 U.S. 1, 10-14 (1972).

For all of the above reasons, the Complaint should be dismissed for lack of standing.

POINT II: CONGRESS IMPLIEDLY PRECLUDED JUDICIAL REVIEW OF PLAINTIFFS' STATUTORY CLAIM

Congress has impliedly precluded judicial review of the type of statutory claim Plaintiffs assert – that is, a claim by telephone subscribers that the provision of telephony metadata to the

Government, pursuant to a FISC order, violates Section 215. *See* Compl. ¶ 36. Thus, Plaintiffs cannot rely on the waiver of sovereign immunity codified in the Administrative Procedure Act (APA), 5 U.S.C. § 702; *see* Compl. ¶ 4, to supply the needed waiver for their statutory claim. The APA's waiver of sovereign immunity does not apply where, as here, Congress has granted consent to suit in specified circumstances or fora, or by specified parties, under another statute, and thus impliedly foreclosed the relief sought. 5 U.S.C. § 702. Nor does the APA authorize suit where "statutes preclude judicial review," as Section 215 clearly does. *Id.* § 701(a)(1). Plaintiffs' statutory claim must therefore be dismissed.

"It is elementary that the United States, as sovereign, is immune from suit save as it consents to be sued . . . ." *United States v. Mitchell*, 445 U.S. 535, 538 (1980) (internal quotations omitted); *see also FDIC v. Meyer*, 510 U.S. 471, 475 (1994) ("Absent a waiver, sovereign immunity shields the Federal Government and its agencies from suit."). "A waiver of sovereign immunity cannot be implied but must be unequivocally expressed." *Mitchell*, 445 U.S. at 538 (internal quotations omitted). Any ambiguity is construed in favor of immunity. *FAA v. Cooper*, 132 S. Ct. 1441, 1448 (2012). Ambiguity exists if there is a "plausible interpretation" of the statute that would *not* authorize the relief sought. *Id*.

As a general matter, section 702 of the APA grants the Government's consent to suit in actions "seeking relief other than money damages." It is subject to a number of significant exceptions, however, two of which apply here. First, section 702 itself provides that "[n]othing herein … confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702. Second, mirroring the first exception, the APA provides that its chapter on judicial review, including section 702, does not apply "to the extent that … statutes preclude judicial review." 5 U.S.C. § 701(a)(1).

The first exception "prevents plaintiffs from exploiting the APA's waiver to evade limitations on suit contained in other statutes." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 132 S. Ct. 2199, 2204-05 (2012). As Congress explained when it enacted the APA's waiver of immunity, this "important carve-out," *id*. at 2204, makes clear that section 702 was "not intended to permit suit in circumstances where statutes forbid or limit the relief sought," that is, where "Congress has consented to suit and the remedy provided is intended to be the exclusive remedy." H.R. Rep. No. 94-1656, at 12-13 (1976), 1976 WL 14066, * 12-13. "For example, . . . a statute granting the United States' consent to suit, i.e., the Tucker Act, 'impliedly forbids' relief other than the [damages] remedy provided by the Act." *Id.* Thus, "'[w]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy'—including its exceptions—to be exclusive, that is the end of the matter; the APA does not undo the judgment." *Pottawatomi Indians*, 132 S. Ct. at 2205 (quoting *Block v. North Dakota ex rel. Bd. of Univ. and Sch. Lands*, 461 U.S. 273, 286, n. 22 (1983)).

To much the same effect, section 701(a)(1) of the APA withdraws section 702's waiver of immunity where "statutes preclude judicial review." § 701(a)(1) ("This chapter applies, according to the provisions thereof, except to the extent that (1) statutes preclude judicial review"). "Whether and to what extent a particular statute precludes judicial review is determined not only from its express language, but also from the structure of the statutory scheme, its objectives, its legislative history, and the nature of the administrative action involved." *Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 345 (1984). "[W]hen a statute provides a detailed mechanism for judicial consideration of particular issues at the behest of particular persons, judicial review of those issues at the behest of other persons may be found to be impliedly precluded." *Id.; see Pottawatomi Indians,* 132 S. Ct. at 2213.

Here, a provision of the USA PATRIOT Act that permits specified suits against the United States impliedly forbids Plaintiffs' statutory claim for equitable relief. Pub. L. No. 107-56, § 223, 115 Stat. 294 (2001), codified at 18 U.S.C. § 2712. Section 2712, titled "Civil actions against the United States," authorizes suits against the United States to recover money damages for willful violations of the Wiretap Act, the Stored Communications Act (SCA), and three particular provisions of FISA. 18 U.S.C. § 2712(a). The three specified provisions of FISA are sections 106(a), 305(a), and 405(a), which respectively impose restrictions on the use and disclosure of information obtained from electronic surveillance, physical searches, and pen registers or trap and trace devices authorized under FISA. *See* 50 U.S.C. §§ 1806(a), 1825(a), 1845(a). Significantly, violations of the parallel "use" provision of Section 215, 50 U.S.C. § 1861(h), which restricts the Government's use and disclosure of tangible things received in response to a production order, are *not* made actionable under section 2712.[6] Congress further stipulated that an action under § 2712 shall be the exclusive remedy against the United States for claims falling within its purview. *Id*. § 2712(d). Section 2712 thus deals with claims for misuses of information obtained under FISA in great detail, including the intended remedy, and Plaintiffs cannot rely on section 702 to bring a claim for violation of FISA's terms that Congress did not provide for under 18 U.S.C. § 2712. *Pottawatomi Indians,* 132 S. Ct. at 2205.

The same conclusion was reached by another district court in a suit challenging alleged NSA "dragnet" surveillance after the 9/11 attacks. *Jewel v. NSA*, 2013 WL 3829405 (N.D. Cal. July 23, 2013). The court in *Jewel* held that § 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United

[6] The enactment of section 223 of the USA PATRIOT Act in 2001 preceded enactment of 50 U.S.C. § 1861(h) in 2006. 1 Kris & Wilson § 19:11 at 718. Congress has not since amended § 2712 to include violations of § 1861(h) as a basis for suit. In fact, when Congress amended Section 215 to add subsection (h), it also added the review provision at subsection (f), but made review available only to persons to whom Section 215 orders are directed.

States that seek injunctive relief under any provision of FISA." *Id.* at *12. Accordingly, the plaintiffs there could not rely on section 702 of the APA as a waiver of sovereign immunity for their FISA-based claim for injunctive relief. *Id*. The same result is required in this case.

Section 215 also reflects an intent by Congress to foreclose the statutory claim asserted here, by this type of plaintiff, in this forum, and thus qualifies as a "statute[] [that] preclude[s] judicial review." 5 U.S.C. § 701(a)(1). Section 215 carefully delineates who may seek review of a production order and in what court, specifying that "[a] person receiving a production order" may challenge its legality "by filing a petition with [the FISC review] pool" to "modify or set [it] aside." 50 U.S.C. § 1861(f)(2)(A)(i), (B). Making the preclusive intent of this provision even clearer, Congress punctuated it with the instruction that "[a]ny production … order not explicitly modified or set aside consistent with [subection 1861(f)]," that is, on pool review of a provider petition, "shall remain in effect." *Id.* § 1861(f)(2)(D). Thus, Congress clearly limited the right to contest the legality of Section 215 production orders to recipients of such orders who file petitions for review with the FISC. Indeed, when Congress authorized providers to petition the FISC for review of Section 215 orders, it rejected an amendment that would have allowed such review in federal district court. *See* H. R. Rep. 109-174 at 128-29, 134, 137. [7]

Like the statutory scheme under § 2712, Section 215 indicates that Congress meant to exclude a suit such as the instant one, brought by parties that are not recipients of a production order, in federal district court, not the FISC, seeking equitable relief in a challenge to the

[7] Further telling is Congress's decision to not authorize motions to suppress information obtained from a Section 215 order. When the United States or a state intends to use evidence obtained or derived from electronic surveillance, physical searches, or use of pen register or trap-and-trace (PR/TT) devices authorized under FISA in judicial or administrative proceedings against a person, FISA permits that person to contest the legality of the evidence through a suppression motion. 50 U.S.C. §§ 1806(e), 1825(f), 1845(e). But tangible things acquired under Section 215 are not the products of electronic surveillance, physical searches, or use of PR/TT devices. *See* 50 U.S.C. § 1801(f) (defining electronic surveillance), § 1821(5) (physical search), § 1841(2) (PR/TT devices).

statutory validity of a Section 215 production order. This limitation on judicial review makes sense, given that the tangible things that are the subject of a Section 215 order belong to the recipients of the production order, not to third parties such as plaintiffs here. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976).[8] This "detailed mechanism for judicial consideration of particular issues" under Section 215 "at the behest of particular persons" means that "judicial review of those issues at the behest of other persons" is "impliedly precluded." *Cmty Nutrition Inst.*, 467 U.S. at 349 (holding that statutory scheme allowing dairy handlers to seek review of milk marketing orders precluded actions by consumers); *see also Dew v. United States*, 192 F.3d 366, 371-74 (2d Cir. 1999) (statute prohibiting employment discrimination on the basis of military service, which authorized civil enforcement action against state and private employers, impliedly precluded suit for equitable relief under the APA by employees of federal intelligence community agencies); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 128-29 (E.D. Va. 2011) (provision of SCA allowing Twitter subscribers to challenge orders requiring production to Government of "backup information" impliedly prohibited statutory challenge by subscribers to order requiring production of electronic records pertaining to them).

For these reasons, Plaintiffs' first cause of action, alleging that the Government has acted in excess of its authority under Section 215, should be dismissed.

POINT III: THE GOVERNMENT'S BULK COLLECTION OF TELEPHONY METADATA IS AUTHORIZED UNDER SECTION 215

Even setting aside the jurisdictional deficiencies described above, the Complaint should still be dismissed for failure to state a claim, because it does not "plausibly suggest" that the

[8] Nor does a party, in the absence of a claim of privilege, typically have standing to object to a subpoena directed to a non-party witness. *Langford v. Chrysler Motors Corp.*, 513 F.2d 1121, 1126 (2d Cir. 1975).

collection of metadata authorized by the FISC either exceeds the bounds of Section 215, or (as discussed in Points IV and V, *infra*) violates the Constitution. *Iqbal*, 556 U.S. at 681.

As their first cause of action Plaintiffs assert that bulk collection of telephony metadata as contemplated by the FISC's Orders exceeds the authority granted by Section 215. Compl. ¶ 36. The Complaint does not set forth the basis for this claim, but, in their July 2, 2013, pre-conference letter to the Court, Plaintiffs suggest that the production ordered by the FISC is unauthorized because (i) the records in question are not "relevant" to an authorized national security investigation, and (ii) Section 215 does not authorize collection of records "as they are generated." Both of these contentions lack merit and should be rejected.

A. The Telephony Metadata Collected Under the FISC's Orders Are "Relevant" to Authorized National Security Investigations

Section 215 authorizes the FISC to order "production of any tangible things" upon the Government's application showing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation … to protect against international terrorism." 50 U.S.C. § 1861(a)(1), (b)(2)(A). As recited in the Secondary Order, at 1, the FBI made such an application for an order directing the production of telephony metadata, and the FISC specifically found, in the Primary Order, at 2, "reasonable grounds to believe" that the telephony metadata sought by the Government "are relevant to authorized investigations … being conducted by the FBI … to protect against international terrorism." Plaintiffs now ask this Court to second-guess the FISC's conclusion and declare instead that the records the FISC ordered produced to the Government are not, in fact, relevant to authorized counter-terrorism investigations, on the apparent ground that the vast majority of those records do not themselves document calls made in connection with terrorist plots. *See* Compl. ¶¶ 2, 30-34. Plaintiffs' position is contrary to Congress's understanding of the term "relevant" under Section 215, the statute's intended purpose, and repeated decisions of the FISC, and should be rejected.

1. Congress Intended Section 215 To Incorporate a Broad Concept of Relevance, Drawn from the Legal Meaning Applied in Grand Jury, Civil, and Administrative Proceedings, That Also Takes Into Account the Special Characteristics of the Terrorism Investigations to Which It Applies

Even in common usage, "relevant" broadly connotes anything "[b]earing on or connected with," or "pertinent to," a specified matter or thing. Oxford English Dictionary (3d ed. 2009) (*available at* www.OED.com). Relevance, however, has developed an even broader legal meaning in the context of official investigations and civil proceedings, for which purposes documents are considered "relevant" not only where they directly bear on a matter, but also where they reasonably could lead to other information that may bear on the matter.

In civil discovery, for example, the phrase "relevant to the subject matter involved in the pending action" broadly encompasses "any matter that bears on, *or that reasonably could lead to other matters that could bear on*, any issue that is or may be in the case." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (emphasis added). An even broader relevance standard applies to grand jury subpoenas, which will be upheld, notwithstanding the incidental production of irrelevant documents, unless "there is 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." *United States v. R. Enters., Inc.*, 498 U.S. 292, 301 (1991) (emphasis added); *In re Grand Jury Proceedings*, 616 F.3d 1186, 1202, 1205 (10th Cir. 2010). Likewise, the statutory authority conferred on administrative agencies to subpoena evidence that is "relevant to [a] charge under investigation" affords them "access to virtually any material that might cast light on the allegations" at issue in an investigation, *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984) (internal quotations omitted), and courts generally defer to an agency's appraisal of what is relevant to the investigation at hand, *see NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006).

In light of that basic understanding of relevance, courts in each of these contexts have categorically authorized the production of entire repositories of records, even when any particular record is unlikely to bear directly on the matter being investigated, where searching a large volume of information is the only feasible means of locating much smaller amounts of critical information within the data that directly bears on the matter under investigation.[9] In the analogous field of search warrants for data stored on computers, courts also permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B).[10] These practices, in a variety of settings, demonstrate the broad understanding of the concept of relevance developed in the context of investigatory information gathering.

Congress incorporated this accepted, broad, and context-dependent legal meaning of the term "relevant" into Section 215. Ordinarily, Congress is presumed to adopt the common understanding of the legal terms it employs. *See NLRB v. Amax Coal Co.*, 453 U.S. 322, 329 (1981) ("Where Congress uses terms that have accumulated settled meaning under either equity or the common law, a court must infer, unless the statute otherwise dictates, that Congress means

---

[9] *See, e.g., In re Subpoena Duces Tecum*, 228 F.3d 341, 350-51 (4th Cir. 2000) (subpoena for 15,000 patient files); *In re Grand Jury Proceedings,* 827 F.2d 301, 305 (8th Cir. 1987) (upholding grand jury subpoenas for records of wire money transfers "involving hundreds of innocent people"); *FTC. v. Invention Submission Corp.*, 965 F.2d 1086 (D.C. Cir. 1992); *Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011) (trust account information for all of law firm's clients held relevant to SEC investigation); *Goshawk Dedicated, Ltd. v. Am. Viatical Servs., LLC,* 2007 WL 3492762 at *1 (N.D. Ga. Nov. 5, 2007) (compelling production of business's entire underwriting database); *In re Adelphia Commc'ns. Corp.,* 338 B.R. 546, 549 and 553 (Bankr. S.D.N.Y. 2005) (permitting inspection of "approximately 20,000 large bankers boxes of business records"); *Medtronic Sofamor Danek, Inc. v. Michelson,* 229 F.R.D. 550, 552 (W.D. Tenn. 2003) (compelling discovery of "approximately 996 network backup tapes … plus an estimated 300 gigabytes of other electronic data).

[10] *See, e.g., United States v. Hill,* 459 F.3d 966, 975 (9th Cir. 2006) (recognizing that "blanket seizure" of the defendant's entire computer system, followed by subsequent review, may be permissible); *United States v. Upham,* 168 F.3d 532, 535 (1st Cir. 1999).

to incorporate the established meaning of these terms").[11] In this case, however, both the text and legislative history confirm that Congress was acutely aware of the accepted legal meaning of relevance when it enacted Section 215's relevance requirement.

When Congress codified the relevance requirement under Section 215, *see* USA PATRIOT Act Improvement Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2006), it was understood that relevance was the equivalent of the "well established standard" applied to grand jury subpoenas, administrative subpoenas, and civil discovery requests. *See* 152 Cong. Rec. S1598, 1606 (Mar. 2, 2006) (statement of Sen. Kyl).[12] Indeed, Congress described the items subject to production under Section 215 as things obtainable by "a subpoena duces tecum issued by a court … in aid of a grand jury investigation" or "any other order issued by a court … directing the production of records or tangible things." 50 U.S.C. § 1861(c)(2)(D). And in codifying the relevance standard applicable here, Congress provided that the Government need only show "reasonable grounds to believe" that the records sought are relevant to an authorized investigation, *id* § 1861(b)(2)(A), thus incorporating, too, the deferential standard of review applied to the Government's relevance determinations when it issues investigatory subpoenas. *See R. Enters., supra* at 21, 498 U.S. at 301; *Am. Med. Response*, 438 F.3d at 193.

---

[11] *See also United States v. Shabani*, 513 U.S. 10, 14 (1994); *McLean v. United States*, 566 F.3d 391, 396 (4th Cir. 2009) ("When Congress directly incorporates language with an established legal meaning into a statute, we may infer that Congress intended the language to take on its established meaning"); *Smith v. Bowersox*, 159 F.3d 345, 347 (8th Cir. 1998) (same).

[12] *See also* 152 Cong. Rec. S1379, 1395 (Feb. 16, 2006) (statement of Sen. Kyl) ("We all know the term 'relevance.' It is a term that every court uses … The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation, and for each and every one of the 335 different administrative subpoenas currently authorized by the United States Code"); 151 Cong. Rec. S13636, 13642 (Dec. 15, 2005) (statement of Sen. Hatch) (the relevance standard incorporated into Section 215 "has been used for years in the issuance of grand jury subpoenas," and is "strictly in the mainstream of American criminal law"); H.R. Rep. No. 109-174, pt. 1 at 131 (statement of Rep. Lungren) ("the standard proposed here is really the relevance standard under which Federal grand juries … operate").

Of course, the case law in the contexts of civil discovery, grand jury subpoenas, and administrative investigations does not involve data acquisition on the scale of the telephony metadata collection authorized by the FISC, because the information gathered in those contexts is sought in aid of focused judicial and administrative proceedings involving identifiable individuals and events. But there are a number of textual and contextual indications that Congress also intended Section 215 to embody a sufficiently flexible standard of relevance to take into account the uniquely important purposes and special characteristics of the national security investigations to which the statute applies.

First, unlike the rules that limit civil discovery to information that is relevant "to the subject matter involved" in a case, Fed. R. Civ. P. 26(b)(1), Section 215 permits the collection of information relevant "to an authorized investigation." 50 U.S.C. § 1861(b)(2)(A). Business records can therefore be relevant to an investigation not merely if they relate to the subject matter of an inquiry, but also if there is reason to believe they are necessary to the application of investigative techniques that will advance its purposes. The bulk collection of telephony metadata is necessary to enable discovery of otherwise hidden connections between individuals suspected of engaging in terrorist activity and unknown co-conspirators with whom they maintain contact in the United States. The metadata records are therefore relevant to FBI investigations whose object is to thwart the plots in which these individuals are engaged before they come to bitter fruition.[13]

---

[13] Notably, when Congress codified the relevance standard in Section 215 it *specifically rejected* proposals to limit its scope so that it would encompass only records pertaining to individuals suspected of terrorist activity. *See* S. 2369, 109th Cong., 2d Sess., § 3 (Mar. 6, 2006); 151 Cong. Rec. S14275-01 (Dec. 21, 2005) (statement of Sen. Dodd) ("Unfortunately, the conference report … maintains the minimal standard of relevance without a requirement of fact connecting the records sought, or the individual, suspected of terrorist activity"). *See also* 152 Cong. Rec. S1598-03 (2006) (statement of Sen. Levin); 152 Cong. Rec. H581-02 (Mar. 7, 2006) (statement of Rep. Nadler).

Second, relevance in the context of national security investigations cannot be evaluated in a vacuum but must be considered in light of their special nature, purpose, and scope. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946). Counter-terrorism investigations serve important purposes beyond the ambit of routine criminal inquiries, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they occur. Hence, national security investigations often have remarkable breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, intended targets, and means of attack, many of which are often unknown to the intelligence community at the outset. *See CIA v. Sims,* 471 U.S. 159, 171 (1985) ("foreign intelligence [gathering] consists of securing all possible data pertaining to … the national defense and security of the United States"). National security investigations thus require more far-reaching means of information-gathering to shed light on suspected terrorist organizations, their size and composition, recruitment, geographic reach, relation to foreign powers, financial resources, past acts, goals, and capacity for carrying out their plans.

When Congress codified the relevance standard under Section 215, the critical differences between the breadth and attributes of counter-terrorism investigations and routine criminal investigations were well understood. *See* H.R. Rep. No. 109-174(1) at 129 (statement of Rep. Lungren) ("[t]his is in the nature of trying to stop terrorists before they act, not in the nature of a regular criminal investigation … and it strikes … precisely at when a 215 order is most useful"); *see also* 152 Cong. Rec. S1325, 1330 (Feb. 15, 2006) (statement of Sen. Feingold). The purpose underlying the USA PATRIOT Act, and Section 215 in particular, was to provide the intelligence community the enhanced investigatory tools needed to bring terrorist activities to light before they culminate in a loss of life and property. *See* H.R. Rep. No. 109-

174, pt. 2 at 4 ("many of the core enhanced authorities of the [Patriot Act] are fundamentally intelligence authorities intended to gather information to counter threats to national security from terrorists"); S. Rep. No. 109-85 at 40 (noting "critical" nature and "broad reach" of authority conferred by Section 215). To achieve this core objective, the Government must have authority to collect records that can produce information revealing previously unknown operatives and activities, and thus detect and prevent terrorist attacks before they are launched. Limiting the reach of Section 215 to specific records bearing directly on known terrorist threats and operatives would inhibit the use of this authority for its intended purposes – detecting unknown terrorist threats – and frustrate the will of Congress.[14]

2. Congress Has Legislatively Ratified the Construction of Section 215 as Allowing for the Bulk Collection of Telephony Metadata Records

Congress's adoption of this expansive understanding of relevance under Section 215 is further confirmed by the fact that Congress had already been notified of the Government's bulk

[14] When it codified Section 215's relevance requirement, Congress simultaneously built protections into the statutory scheme not found in the other legal contexts. Section 215's requirement for prior judicial authorization – not required for grand jury subpoenas, administrative subpoenas, or civil discovery – serves as a check on the broad investigatory powers granted to the Government in counter-terrorism investigations. For example, the Government's authority to collect telephony metadata must be renewed by the FISC every 90 days, and, pursuant to statutory minimization requirements, the FISC's orders require reasonable, articulable suspicion that identifiers (*e.g.,* telephone numbers) used to query the data are associated with specific foreign terrorist organizations that have previously been identified to and approved for targeting by the Court. *See* Primary Order at 7. Moreover, once information is produced under a Section 215 order, the Government can retain and disseminate it only in accordance with minimization procedures reported to and approved by the Court. *See* 50 U.S.C. § 1861(c)(1), (g). The entire process is subject to active congressional oversight. *See, e.g.*, *id.* § 1862. These multiple and interlocking layers of oversight and regulation further reflect a recognition on Congress's part of the broad authority conferred by Section 215 to gather information "relevant" to a counter-terrorism investigation, and the need for correspondingly robust safeguards to promote responsible use of that authority.

As recent disclosures by the Government demonstrate, *see* n. 5, *supra,* this system of interactive administrative, judicial, and legislative safeguards has succeeded in identifying and correcting issues of unauthorized access to telephony metadata when they have arisen.

collection of telephony metadata when it twice re-authorized Section 215, without change, in 2010 and 2011. Pursuant to – indeed, well beyond – FISA's Congressional notification requirements, *see* 50 U.S.C. 1871(a), the Executive Branch worked to ensure that *all* Members of Congress had access to information about this program and the legal authority for it. In December 2009, a classified briefing paper, explaining that the Government and the FISC had interpreted Section 215 to authorize the bulk collection of telephony metadata, was provided to the House and Senate Intelligence Committees and made available for review, as well, by all Members of Congress, "to inform the legislative debate about reauthorization of Section 215." [15] Additionally, the classified use of this authority has been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, including in connection with reauthorization efforts, as several Members of Congress have acknowledged.[16]

---

[15] *See* Letter from Ronald Weich to the Hon. Silvestre Reyes (Dec. 14, 2009) (Exh. 4, hereto); Report on the [NSA's] Bulk collection Programs for USA PATRIOT Act Reauthorization (Exh. 5, hereto). Both Intelligence Committees made this document available to all Members of Congress prior to the February 2010 reauthorization of Section 215. *See* Letter from Sens. Feinstein and Bond to Colleagues (Feb. 23, 2010) (Exh. 6, hereto); Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (Exh. 7, hereto); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden).

An updated version of the briefing paper, *see* Exhibit 8, hereto, was provided to the Senate and House Intelligence Committees again in February 2011 in connection with the reauthorization that occurred later that year. *See* Letter from Ronald Weich to Hon.Diane Feinstein and the Hon. Saxby Chambliss (Feb. 2, 2011) (Exh. 9, hereto); Letter from Ronald Weich to the Hon. Mike Rogers and the Hon. C.A. Dutch Ruppersberger (Feb. 2, 2011) (Exh. 10, hereto). The Senate Intelligence Committee made this updated paper available to all Senators later that month. *See* Letter from Sens. Feinstein and Chambliss to Colleagues (Feb. 8, 2011).

The Court may judicially notice these records and correspondence concerning the legislative history of Section 215's reenactment. *Oneida Indian Nation of N.Y. v. State of New York,* 691 F.2d 1070, 1086 (2d Cir. 1982).

[16] *See* Press Release of Sen. Select Comm. on Intelligence (June 6, 2013) (Exh. 11, hereto) ("The … use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each reauthorization of this law."); *How Disclosed NSA Programs*

After receiving these classified briefings, Congress twice reauthorized Section 215, in 2010 and again in 2011.[17] "'Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.'" *Forest Grove Sch. Dist. v. T.A.*, 557 U.S. 230, 239-40 (2009) (quoting *Lorillard v. Pons*, 434 U.S. 575, 580 (1978)). That presumption is ironclad in this instance, where Congress had actual and repeated notice of the Executive Branch's administrative construction of Section 215 over a period of years.[18] Imposing a limiting construction now on Section 215's relevance standard that would prohibit bulk collection of telephony metadata would be contrary to the express understanding of the statute that Congress ratified on two separate occasions.

3. Telephony Metadata Are "Relevant" Within the Meaning of Section 215 Because Bulk Collection of the Data Enhances the Government's Ability To Detect Terrorist Operatives and Prevent Terrorist Attacks

Acknowledging the intended scope of Section 215 is not to say that the authority it confers is boundless. The Government's ability to analyze telephony metadata to discover connections between individuals fundamentally distinguishes such data from other information,

---

Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the House Perm. Select Comm. on Intelligence 2, 35, 58, 113th Cong., 1st Sess. (2013) (statements of Reps. Rogers, Langevin, and Pompeo) (Exh. 12, hereto).

[17] USA PATRIOT Act – Extension of Sunsets, Pub. L. No. 111-141, § 1(a), 124 Stat. 37; PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216.

[18] *See Atkins v. Parker*, 472 U.S. 115, 140 (1985) ("Congress was thus well aware of, and legislated on the basis of, the contemporaneous administrative practice . . . and must be presumed to have intended to maintain that practice absent some clear indication to the contrary"); *Shell Oil*, 466 U.S. at 69; *Haig v. Agee*, 453 U.S. 280, 297-98 (1981).

Moreover, in both 2009 and 2011, when the Senate Judiciary Committee was considering possible amendments to Section 215, it made clear that it had no intention of affecting the telephony metadata collection program. The Committee reports accompanying the USA PATRIOT Act Sunset Extension Acts of 2009 and 2011 explained that proposed changes to Section 215 were "not intended to affect or restrict any activities approved by the FISA court under existing statutory authorities." S. Rep. No. 111-92, at 7 (2009); S. Rep. No. 112-13, at 10 (2011). Ultimately, Section 215 was extended to June 1, 2015 without change. *See* Patriot Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (2011).

such as library or medical records. For example, while an identified suspect's medical history might be relevant to an investigation of that individual, searching an aggregate database of medical records—which do not interconnect with one another—would not typically enable the Government to identify otherwise unknown relationships among individuals and organizations and thereby ascertain information about terrorist networks. Ordinarily, therefore, bulk collection of such records would not meet the "relevance" standard. *See Okla. Press,* 327 U.S. at 209 (explaining that "relevancy and adequacy or excess in the breadth of [a] subpoena are matters variable in relation to the nature, purposes and scope of the inquiry").

But in light of Congress's broad understanding of "relevance" under Section 215 as it necessarily applies to national security investigations, and Congress's repeated, informed decisions to reauthorize the statute without change, the telephony metadata collection clearly meets the Section 215 "relevance" standard, as the judges of the FISC have repeatedly found. Collecting these data is necessary to the effective use of NSA analytical tools, which, when applied to the data, produce information that can help identify clandestine terrorist operatives or networks within the United States. That process is not feasible without bulk collection of the data, because NSA analysts cannot know in advance which of the many phone numbers obtained might have connections to known or suspected terrorists. And unless the telephony metadata are aggregated and retained for appropriate periods, it may not be feasible to identify chains of communications that cross different time periods and telecommunications networks. Thus, the telephony metadata records are "relevant" to authorized investigations of international terrorism.

B. Nothing in the Text of Section 215 Prohibits the Collection of Records "as They Are Generated"

Plaintiffs' next contention, that Section 215 authorizes only the collection of business records "already in existence," and not the production of records "as they are generated," July 3, 2013, Letter at 3, is erroneous as a matter of law.

Section 215 authorizes the FISC to direct the production of "*any* tangible things," "documents," or "records." 50 U.S.C. § 1861(a)(1)(emphasis added). Nothing in the text of the statute suggests that FISC orders may apply only to records previously created. That requested information is not created until after a FISC order has been rendered, and is produced on an ongoing basis, does not affect its basic character as "documents," "records," or other "tangible things" subject to production under the statute. Nor do the FISC's orders require the creation or preservation of documents that would otherwise not exist, or compel telecommunications service providers to retain information they would otherwise discard. For example, telephony metadata such as the information at issue here is routinely maintained by providers for at least 18 months pursuant to Federal Communications Commission regulations. *See* 47 C.F.R. § 42.6.

Prospective production of business records has been deemed appropriate in analogous contexts. For example, under the SCA the Government may obtain a court order requiring a provider of cell-phone service to produce non-content "record[s] or other information pertaining to a subscriber … or customer" on a specific showing of "reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(c)(1), (d). Courts including this one have held that the Government may seek prospective disclosure of records under the SCA because "the prospective … information sought by the Government … becomes a 'historical record' as soon as it is recorded by the provider," and the statute "in no way limits the ongoing disclosure of records to the Government as soon as they are created." *In re Application of the United States,* 632 F. Supp. 2d 202, 207 n.8 (E.D.N.Y. 2008); *In re Application of the United States*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) (the SCA "contains no explicit limitation on the disclosure of prospective data"). Like the SCA, there is nothing in the text or legislative history of FISA indicating that Congress meant to prohibit the contemporaneous production to the Government

of business records that are generated on a daily basis.[19] Any contention otherwise fails as a matter of law.

POINT IV: THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA DOES NOT VIOLATE PLAINTIFFS' FOURTH AMENDMENT RIGHTS

Plaintiffs also fail to state a claim that the collection of telephony metadata pursuant to the FISC's Orders violates their Fourth Amendment rights. *See* Compl. ¶ 37. The Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that there is no reasonable expectation of privacy in this exact kind of information – dialed telephone numbers – and therefore the Fourth Amendment is not implicated here. Moreover, even if the Fourth Amendment were applicable, the production of metadata ordered by the FISC would satisfy the reasonableness standard applicable to suspicionless searches that serve special government needs, in which the intrusion on privacy interests is balanced against the Government's interest in the search. Here, the collection of metadata is minimally intrusive despite its breadth, as the data include no content, and the FISC's Orders impose restrictions on both access to the data and their dissemination. On the other hand, the metadata collection promotes a governmental interest of the utmost importance – thwarting terrorist attacks.

A. Plaintiffs Have No Fourth Amendment Privacy Interest in Telephony Metadata

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." As the Supreme Court remarked just last year, "for most of our history the

---

[19] This type of prospective order also provides efficient administration for all parties involved—the Court, the Government, and the provider. There is little doubt that the Government could seek a new order on a daily basis for the records created within the last 24 hours, but doing so would unnecessarily burden the Court, the Government, and providers alike. Prospective orders merely ensure that the records can be sought in a reasonable manner for a reasonable period of time while avoiding unreasonable and burdensome paperwork.

Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S. Ct. 945, 949-50 (2012). In addition to the core concern over searches and seizures within these enumerated areas, it is now understood that a Fourth Amendment "search" takes place when the government's investigative activities "violate a person's 'reasonable expectation of privacy.'" *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967)).

The Government's collection of telephony metadata under the FISC's Orders does not involve a "search" of individual telephone subscribers or their property. The Orders are directed to telecommunications service providers, not to subscribers, and direct the production of what are indisputably the providers' own business records. Nor do telephone subscribers have a reasonable expectation of privacy in telephony metadata. In *Smith v. Maryland,* the Supreme Court held that the government's recordation of numbers dialed from an individual's home telephone, through a pen register installed at the telephone company's central offices, did not constitute a search of that individual under the Fourth Amendment, because persons making telephone calls, even from their own homes, lack a reasonable expectation of privacy in the numbers they call. 442 U.S. at 741-46. In contrast to the contents of telephone calls, the Court held that there is no reasonable expectation of privacy in the telephone numbers dialed, because telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes," such as billing and fraud detection. *Id*. at 743.

Furthermore, the Court reasoned, even if a subscriber harbored a subjective expectation that the phone numbers he dialed would remain private, such an expectation of privacy would not be reasonable, because "a person has no legitimate expectation of privacy in information he

voluntarily turns over to third parties." *Id.* at 743-44. The Court explained that someone who uses a phone has "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore has "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744. Courts have followed *Smith* to find no reasonable expectation of privacy in email "to/from" and Internet protocol ("IP") addressing information, *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008); *In re Application of the United States*, 830 F. Supp. 2d at 131-38, in text message addressing information, *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds*, 130 S. Ct. 2619 (2010), and in subscriber information, such as subscribers' names, addresses, birthdates, and passwords, communicated to system operations and Internet service providers, *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

Smith is fatal to Plaintiffs' claim that the collection of metadata records of their communications violates the Fourth Amendment. So far as metadata include such information as the times and duration of their calls and the numbers of the parties with whom they spoke, that is information that telephone subscribers voluntarily turned over to their providers. The remaining data, such as trunk identifiers, is information generated by the phone companies themselves. *See* Primary Order at 3 n.1. Call-detail records memorializing this information belong to the phone companies, as the parties providing the equipment and services required to make those calls possible. *See United States v. Miller*, 425 U.S. at 440-41 (rejecting a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, inasmuch as the bank was a party to the transactions, the records belonged to the bank). Thus, under *Smith*, there can be no reasonable expectation of privacy in this information, even if – as has not been alleged here – there were an understanding that the third party (*i.e.*, the telephone company) would treat the

information as confidential. *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *Miller*, 425 U.S. at 443 ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party … even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

Plaintiffs' July 2, 2013, pre-conference letter cites *Jones* for the proposition that metadata collection "over long periods" constitutes a Fourth Amendment search, but *Jones* is inapplicable here. *Jones* held that "the Government's installation of a GPS [tracking] device on a [targeted individual's] vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" 132 S. Ct. at 949. The Court reached that conclusion on the basis of considerations that are entirely absent here – namely, attachment of a tracking device to an individual's vehicle to collect track his whereabouts, thus effecting a physical intrusion on that person's "effects," one of the spheres that the Fourth Amendment explicitly enumerates as protected. *Id.* ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information"). The collection of telephony metadata, unlike affixing a GPS device to a vehicle, does not involve any trespass or other intrusion on Plaintiffs' property, or tracking of locations from which telephone calls are made.

Moreover, contrary to Plaintiffs' contentions, the majority in *Jones* expressly disclaimed reliance on the duration of the monitoring (a factor on which the court below had relied, *see United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2012)), as a basis for concluding that a search had occurred. 132 S. Ct. at 954; *see also United States v. Anderson-Bagshaw*, 2012 WL 774964, at *2 (N.D. Ohio. Mar. 8, 2012) ("The [*Jones*] majority limited its analysis to the trespassory nature of the GPS installation, refusing to establish some point at which uninterrupted surveillance might become constitutionally problematic.").

Nor does the scope of the metadata collection under the FISC's Orders alter the Fourth Amendment analysis. Fourth Amendment rights "are personal in nature, and cannot bestow vicarious protection on those who do not have a reasonable expectation of privacy in the place to be searched." *Steagald v. United States*, 451 U.S. 204, 219 (1981); *accord, e.g.*, *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (a person "claim[ing] the protection of the Fourth Amendment … must demonstrate that he personally has an expectation of privacy in the place searched"); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978) (Fourth Amendment rights are personal rights which may not be vicariously asserted). No Fourth Amendment-protected interest of Plaintiffs is implicated, therefore, by virtue of the fact that the metadata records of many other individuals' calls are collected as well as their own. *See In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) (rejecting argument that a subpoena was unreasonable under the Fourth Amendment because it "may make available to the grand jury [money transfer] records involving hundreds of innocent people"); *United States v. Rigmaiden*, 2013 WL 1932800, at * 13 (D. Ariz. May 8, 2013) (Government did not violate defendant's Fourth Amendment rights by acquiring a high volume (1.8 million) of IP addresses).

B. The Government's Acquisition of Metadata Is Reasonable

Even if collecting telephony metadata involved a Fourth Amendment "search" (it does not), the Fourth Amendment bars only "unreasonable" searches and seizures, whereas the collection of metadata at issue here is reasonable under the standard the Supreme Court applies to assess suspicionless searches that serve special government needs. That standard requires a court to balance "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted); *see also Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995). That balance overwhelmingly favors the Government here.

First, if, contrary to *Smith*, Plaintiffs could be said to have any Fourth Amendment privacy interest that is implicated by collection of non-content telephony metadata, that interest would be minimal. Moreover, the intrusion on that interest would be mitigated still further by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC's Primary Order, at 4-14. *See King*, 133 S. Ct. at 1979 (safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 833 (2002) (restrictions on access to drug testing results lessened intrusion on privacy); *Vernonia Sch. Dist.*, 515 U.S. at 658 (intrusion of urine-testing on student athletes' privacy was significantly reduced by the fact that they were tested only for illegal drugs and not for any medical condition).

On the other side of the balance, the collection and analysis of telephony metadata promotes overriding public interests. The Government's interest in identifying and tracking terrorist operatives for the purpose of preventing terrorist attacks is a national security concern of overwhelming importance. *See Haig*, 453 U.S. at 307 ("no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); *In re Directives*, 551 F.3d 1004, 1012 (FISC-R 2008) ("the relevant governmental interest – the interest in national security – is of the highest order of magnitude."); *United States v. Smith*, 426 F.3d 567, 573 (2d Cir. 2005). Bulk collection of telephony metadata is a "reasonably effective means" of promoting the Government's national security objectives, *Earls*, 536 U.S. at 837, inasmuch as accumulating metadata enhances the Government's ability to uncover and monitor unknown terrorist operatives who could otherwise elude detection.[20] Given that the Government's

[20] The Government need not show that it is using the least intrusive means available to accomplish its goal, *id.*; *United States v. Martinez-Fuerte*, 428 U.S. 543, 556 n. 12 (1976), and a low percentage of positive outcomes among the total number of searches or seizures does not render a program ineffective. *See Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 454 (1990)

collection of metadata serves exceedingly important public interests, with minimal, if any, intrusion on the privacy of telephone subscribers, it would be constitutional even if the Fourth Amendment's reasonableness standard applied.

For these reasons, the Plaintiffs' Fourth Amendment claim should be dismissed.

POINT V: PLAINTIFFS HAVE NOT PLAUSIBLY ALLEGED THAT THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA VIOLATES THE FIRST AMENDMENT

Plaintiffs' final claim, that FISC-authorized collection of telephony metadata violates the First Amendment, Compl. ¶ 38, perishes in the wake of their failed Fourth Amendment claim. The law is clear that governmental investigations conducted in observance of Fourth Amendment requirements, without purpose to deter or penalize protected expression or association, do not violate the First Amendment. Plaintiffs do not allege that the Government's collection of telephony metadata is intended for any purpose other than to identify terrorist operatives, and prevent terrorist attacks. Accordingly, their First Amendment claim should be dismissed.

A. Plaintiffs' Failure to Allege an Actionable Fourth Amendment Claim Is Also Fatal to Their First Amendment Claim

Plaintiffs allege the same injury in support of their First Amendment claim as their Fourth Amendment claim: that telephony metadata collected under the FISC's Orders gives the Government the wherewithal to piece together "a comprehensive record" of "sensitive" information about Plaintiffs and their associations that is "likely to have a chilling effect on people who would otherwise contact Plaintiffs" for purposes related to Plaintiffs' organizational mission. Compl. ¶¶ 1, 3, 35. Thus, Plaintiffs' putative First Amendment claim is at best

---

(detention of 126 vehicles entering a highway sobriety checkpoint resulted in arrest of two drunken drivers); *Martinez-Fuerte*, 428 U.S. at 554 (out of 146,000 vehicles passing through border checkpoint, 171 were found to contain deportable aliens). Government officials are given a degree of latitude and deference in choosing among reasonable alternatives in structuring a program involving suspicionless search or seizure. *Sitz*, 496 U.S. at 453-54.

derivative of their Fourth Amendment claim. *See, e.g.*, *ACLU v. NSA*, 493 F.3d 644, 657 (6th Cir. 2007) (opinion of Batchelder, J.) (observing that plaintiffs who challenged alleged warrantless wiretapping by NSA on various constitutional grounds "have only one claim, namely, breach of privacy, based on a purported violation of the Fourth Amendment or FISA … On a straightforward reading, this claim does not implicate the First Amendment.").

The Supreme Court and every court of appeals to consider the issue have concluded that when governmental investigative activities have an impact on the exercise of First Amendment freedoms, those interests are safeguarded by adherence to Fourth Amendment standards. *See, e.g.*, *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *United States v. Mayer*, 503 F.3d 740, 747-48 (9th Cir. 2007).[21] Accordingly, "surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities." *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases).[22] Inasmuch as Plaintiffs have failed to state a claim under the Fourth Amendment, this precedent alone requires dismissal of Plaintiffs' First Amendment claim, too. *Reporters Comm.*, 593 F.2d at 1059; *see also Mayer*, 503 F.3d 750 (similar); *United States v. Gering*, 716 F.2d 615, 620 (9th Cir. 1983) (rejecting surveilled party's argument that First Amendment afforded him an expectation of privacy where the Fourth Amendment would not); *ACLU v. NSA*, 493 F.3d at 657 (similar).

---

[21] *See also Redd v. City of Enter.*, 140 F.3d 1378, 1383 (11th Cir. 1998); *Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1055-59 (D.C. Cir. 1978); *Jabara v. Kelley*, 476 F. Supp. 561, 572 (E.D. Mich. 1979) (the First and Fourth Amendments "provide coextensive zones of privacy in the context of a good faith criminal investigation," including warrantless electronic surveillance), *vacated on other grounds*, 691 F.2d 272 (6th Cir. 1982).

[22] *See Mayer*, 503 F.3d at 750 (same); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991) (same in context of FISA surveillance). *See also United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (where mail is subject to inspection by customs officers only when they have "reasonable cause to suspect" it contains something other than correspondence, and the correspondence may not be read absent a warrant, the First Amendment is not violated).

B. Plaintiffs Make No Allegations That the Government's Collection of Telephony Metadata Is Intended to Curtail Protected Expressive or Associational Activity

Plaintiffs' First Amendment claim is also subject to dismissal because it is based solely on the alleged incidental effects of good-faith investigatory conduct. "Not every Government action that affects, has an impact on, or indeed inhibits First Amendment activity constitutes the kind of 'abridgement' condemned by the First Amendment." *Reporters Comm.*, 593 F.2d at 1052; *see also City Council of Los Angeles v. Taxpayers for Vincent,* 466 U.S. 789, 803-04 (1984). Courts have long recognized the need, even when summoned to action in the name of constitutionally protected rights, to accommodate the Government's competing interests where prevention of crime, or, even more imperatively, potential threats to national security are concerned. *See, e.g.*, *Socialist Workers Party v. Attorney General*, 510 F.2d 253, 256 (2d Cir. 1974) ("The FBI has a right, indeed a duty, to keep itself informed with respect to the possible commission of crimes; it is not obliged to wear blinders until it may be too late for prevention.").

Accordingly, courts distinguish for purposes of First Amendment analysis between government investigations that may have the incidental effect of deterring First Amendment activity, and concrete government action of a regulatory, proscriptive, compulsory, or intrusive nature that is specifically directed against individuals or organizations based on their expressive or associational activities. *See, e.g.*, *Zurcher*, 436 U.S. at 564; *Laird*, 408 U.S. at 11; *Reporters Comm.*, 593 F.2d at 1051-55. Otherwise lawful investigative activities conducted in good faith—that is, "not for the purpose of abridging first amendment freedoms," *United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989)—do not violate the First Amendment. *See Reporters Comm.*, 593 F.2d at 1051 (concluding that First Amendment protects activities "*subject to* the general and incidental burdens that arise from good faith enforcement of otherwise valid criminal and civil laws that are not themselves solely directed" at First Amendment conduct).

Here, Plaintiffs advance no claim that the Government's collection and analysis of telephony metadata has any objective other than furthering the compelling national interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks. The Complaint certainly contains no allegations, well-pled or otherwise, from which it could plausibly be concluded that the Government's collection of non-content telephony metadata is aimed at curtailing any First Amendment expressive or associational activities. To the contrary, the Complaint's allegations regarding the authorized breadth of the collection, Compl. ¶¶ 30-34, highlight the fact that it is undertaken without targeting Plaintiffs or any other persons, and without reference to anyone's conduct protected by the First Amendment. Plaintiffs have thus failed to state a First Amendment claim that plausibly gives rise to an entitlement to relief. *Iqbal*, 556 U.S. at 678-79; *see Reporters Comm.*, 593 F.2d at 1052 ("[T]he Government's good faith inspection of [telephone] toll call records does not infringe on plaintiffs' First Amendment rights, because that Amendment guarantees no freedom from such investigation.").

CONCLUSION

For the reasons stated above, the Court should dismiss the complaint.

Dated: New York, New York
August 26, 2013

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

By: /s/ James Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

Civil Division,
Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
Tel.: (202) 514-3358

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David S. Jones
DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel. (212) 637-2739/2746/2716/2728
Fax (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov