STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205; Fax: (202) 616-8470

Attorneys for the Government Defs. in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 3:13-cv-03287-JSW **GOVERNMENT DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS; OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT** Date: April 25, 2013 Time: 9:00 a.m. Courtroom: 11 – 19th Floor Judge Jeffrey S. White

NOTICE OF MOTION

PLEASE TAKE NOTICE that, on April 25, 2013 at 9:00 a.m, before Judge Jeffrey S. White, Defendants NATIONAL SECURITY AGENCY; KEITH B. ALEXANDER, Director of the NSA, in his official capacity; the UNITED STATES DEPARTMENT OF JUSTICE and ERIC HOLDER, the Attorney General, in his official capacity; Acting Assistant Attorney General for National Security JOHN P. CARLIN, in his official capacity; the FEDERAL BUREAU OF INVESTIGATION and JAMES B. COMEY, Director of the FBI, in his official capacity; and JAMES R. CLAPPER, Director of National Intelligence, in his official capacity (hereafter the "Government Defendants") will move to dismiss the claims in the First Amended Complaint pursuant to Rule 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, and will also oppose the motion for partial summary judgment filed by Plaintiffs pursuant to Rule 56 of the Federal Rules of Civil Procedure. The grounds for this motion and opposition are as follows:

1. The Court lacks subject matter jurisdiction with respect to all claims because Plaintiffs' First Amended Complaint fails to establish their standing to sue, and Plaintiffs have adduced no evidence in support of their motion for partial summary judgment that establishes their standing in fact.

2. The Court lacks subject matter jurisdiction with respect to Plaintiffs' claim that the Government's alleged conduct exceeds its statutory authority under the Foreign Intelligence Surveillance Act because such a claim is precluded by statute.

3. The First Amended Complaint fails to state claims upon which relief can be granted that the Government's alleged conduct exceeds its statutory authority under the Foreign Intelligence Surveillance Act, that the Government's alleged conduct violates the First, Fourth, and Fifth Amendments, or that Plaintiffs are entitled to a return of property under Federal Rule of Criminal Procedure 41(g).

4. The Court should also deny partial summary judgment with respect to Plaintiffs' aforementioned statutory and First Amendment claims—the only claims as to which Plaintiffs have moved for summary judgment—for the reasons stated above, and because (a) Plaintiffs'

have failed to adduce sufficient evidence to establish that the Court has subject matter jurisdiction over such claims; and (b) Plaintiffs have failed to adduce sufficient evidence to establish essential elements of such claims.

The grounds for this motion and opposition, where applicable, are set forth in the accompanying (i) Memorandum of Points and Authorities in Support of the Government Defendants' Motion to Dismiss and Opposition to Plaintiffs' Motion for Partial Summary; and (ii) Exhibits A through R, as set forth in the Declaration of James J. Gilligan, filed herewith.

Dated: December 6, 2013

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director
tony.coppolino@usdoj.gov

/s/ Marcia Berman
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities

STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205; Fax: (202) 616-8470

Attorneys for the Government Defs. in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 3:13-cv-03287-JSW **GOVERNMENT DEFENDANTS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF THEIR MOTION TO DISMISS AND OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

RULES AND REGULATIONS

LEGISLATIVE MATERIALS

FEDERAL RULES OF CIVIL PROCEDURE

FEDERAL RULE OF CRIMINAL PROCEDURE

MISCELLANEOUS

INTRODUCTION

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. The Government's exploitation of terrorist communications is a critical tool in this effort. Plaintiffs in this case seek to invalidate an important means by which the National Security Agency (NSA), acting under authority of the Foreign Intelligence Surveillance Court (FISC), has gathered information about communications among known and unknown terrorist actors in order to thwart future terrorist attacks.

Specifically, Plaintiffs challenge the NSA's collection, under a provision of the Foreign Intelligence Surveillance Act (FISA) known as Section 215, of bulk "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 FISC as consistent with governing law, and constitutional, permits 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 assert that this activity is unauthorized by FISA, and violates the First, Fourth, and Fifth 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 First Amended Complaint should be dismissed, and Plaintiffs' motion for partial summary judgment on their statutory and First Amendment claims should be denied.

First, Plaintiffs fail to establish their standing to sue. The FISC's orders limit review of the metadata for intelligence purposes to records with connections to identifiers (e.g., telephone numbers) that are believed, based on reasonable, articulable suspicion, to be associated with foreign terrorist organizations approved for targeting by the FISC. This requirement bars the type of indiscriminate querying of the metadata, using identifiers not connected with terrorist activity, to create comprehensive profiles of ordinary Americans' associations, as Plaintiffs

speculate. There is no non-speculative basis, then, 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. Plaintiffs' allegations that records of their calls could be used to glean the identities of their members, constituents, and others who wish their association with Plaintiffs to remain confidential, and that such persons are "chilled" by that prospect from contacting them, at most state an injury attributable to misperceptions and conjecture about the Government's activities, but not one fairly traceable to the Government's actual conduct. Second, Plaintiffs' contention that the Government's alleged conduct exceeds its statutory authority under FISA is precluded, *inter alia*, by FISA's detailed scheme for judicial review of specified intelligence activities. In any event, as the FISC has repeatedly (and twice recently) found, the Government's bulk collection of telephony metadata is lawful under FISA because there are reasonable grounds for believing that such data as a whole are relevant to authorized FBI counter-terrorism investigations. Contrary to Plaintiffs' contentions, this collection is not prohibited by the Stored Communications Act, and nothing in Section 215 bars the FISC from prospectively directing the production of electronic business records as they are created.

Third, the Government's collection of telephony metadata is constitutional, and Plaintiffs make no showing to the contrary. Plaintiffs fail to state a Fourth Amendment claim because, consistent with the FISC's repeated holdings, 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. Plaintiffs also fail to state a First Amendment claim, primarily because good faith intelligence-gathering conducted in a manner consistent with the Fourth Amendment, without purpose to deter or punish protected speech or association, does not violate the First Amendment. No parallel can be drawn between the intelligence-gathering activities Plaintiffs seek to put at issue here and cases in which individuals or organizations were compelled to

disclose personally identifying information, or membership lists, based on their protected associational activities. Nor, for purposes of their summary judgment motion, have Plaintiffs met their burden of establishing a prima facie case of infringement of their associational freedoms. Finally, Plaintiffs' due process claims fail for want of a constitutionally protected privacy interest in telephony metadata, and even assuming such an interest exists, it does not entitle them to notice of the Government's intelligence-gathering activities that could undermine the Government's compelling interest in preventing terrorist attacks.

STATEMENT OF FACTS

I. Statutory Background

Congress enacted FISA to authorize and regulate certain governmental surveillance of communications and other activities 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 FISA's "business records" provision, 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." 50 U.S.C. § 1861(a)(1). The Government's application 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 production order once it is granted, but only in limited circumstances. Specifically, it allows "[a] person receiving a production order [to] challenge [its] legality" by filing a petition with the "review pool" of FISC judges designated under 50 U.S.C. § 1803(e)(1) to review such orders. *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). Either the Government or a recipient of a production order may appeal the decision of the pool judge to the FISA Court of Review, with review available thereafter on writ of certiorari in the Supreme Court. *Id.*; *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 D. Kris & J. Wilson, National Security Investigations & Prosecutions §§ 5:5, 19:7 (2d ed. 2012) (Kris & Wilson). The FISA does not provide for review of Section 215 orders at the behest of third parties.

II. The Collection and Analysis of Bulk Telephony Metadata Authorized by the FISC

Plaintiffs here challenge the NSA's FISC-authorized collection and analysis of bulk telephony metadata to discover communications with and among unknown terrorist operatives. Under this program, the Federal Bureau of Investigation (FBI) obtains orders from the FISC pursuant to Section 215 directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of certain "call detail records, or 'telephony metadata,'"

created by the recipient providers for calls to, from, or wholly within the United States. The NSA then stores, queries, and analyzes the metadata for counter-terrorism purposes. Under the FISC's orders, the NSA's authority to continue the program expires after approximately 90 days and must be renewed. The FISC first authorized the program in May 2006, and since then has renewed the program thirty-four times, under orders issued by fifteen different FISC judges.[1]

Under the FISC's orders, telephony metadata is defined 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 terms of the FISC's orders, "[t]elephony metadata does not include the name, address, or financial information of a subscriber or customer" or any party to a call. *Id*.; Secondary Order at 2. Nor do the FISC's orders permit the Government, under this program, to listen to or record the contents of any telephone conversations. Shea Decl. ¶¶ 7, 14-15, 18; Skule Decl. ¶¶ 7, 11.

The Government obtains these orders by submitting detailed applications from the FBI explaining that the records are sought for investigations to protect against international terrorism that concern specified foreign terrorist organizations identified in each application. Skule Decl. ¶ 10; *see* 50 U.S.C. § 1861(a)(1), (b)(2)(A). As required by Section 215, the application contains a statement of facts showing that there are reasonable grounds to believe that the metadata as a whole are relevant to these investigations, supported by a declaration from a senior official of NSA's Signals Intelligence Directorate. Skule Decl. ¶ 10. FISC orders authorizing collection of the metadata are predicated on the Court's findings that there are "reasonable grounds to believe

[1] Declaration of Teresa H. Shea (Shea Decl.) ¶¶ 13-14, 16-17, 20 (Exh. A); Declaration of Joshua Skule (Skule Decl.) ¶¶ 3, 6 (Exh. B); *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR13-109 (F.I.S.C. Aug. 29, 2013) (Aug. 29 FISC Op.) (Exh. C) at 29; *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR 13-158 (F.I.S.C. Oct. 11, 2013) (Oct. 11 FISC Mem.) (Exh. D) at 2-6; *see also In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR13-80, Primary Order (F.I.S.C. Apr. 25, 2013) (Primary Order) (Exh. E) at 3-4, 17; *In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR13-80 (F.I.S.C. Apr. 25, 2013) (Secondary Order) (Exh. F) at 1-2, 4.

that the [records] sought are relevant to authorized investigations . . . being conducted by the FBI . . . to protect against terrorism." *See* Primary Order at 1-2; Aug. 29 FISC Op. at 28.

As also required by Section 215, the FISC's orders direct the Government to comply with "minimization procedures" that strictly limit access to and review of the metadata, and limit dissemination of information derived from the data, to valid counter-terrorism purposes. *See* 50 U.S.C. § 1861(b)(2)(B), (g), (h); Primary Order at 4-17; Skule Decl. ¶ 8; Shea Decl. ¶¶ 29-35. Under these restrictions, NSA analysts may access the metadata only for purposes of obtaining foreign intelligence information, and may do so only through "contact-chaining" queries (electronic term searches) of the metadata using identifiers (typically telephone numbers) approved as "seeds" by one of twenty-two designated officials in NSA's Signals Intelligence Directorate. Such approval may only be given upon a determination that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that a selection term used to query the database is associated with one or more foreign terrorist organizations previously identified to and approved for targeting by the FISC. Where the selection term is reasonably believed to be used by a U.S. person, NSA's Office of General Counsel must also determine that the term is not regarded as associated with a foreign terrorist group solely on the basis of activities protected by the First Amendment. These determinations are effective for finite periods of time. Shea Decl. ¶¶ 19-23, 31; Primary Order at 6-9. This "reasonable, articulable suspicion" requirement bars the indiscriminate querying of the telephony metadata based on identifiers not connected with terrorist activity. Indeed, because of this requirement, the vast majority of the data obtained under this program are never seen by any person; only the tiny fraction of the records responsive to queries authorized under the "reasonable, articulable suspicion" standard are reviewed or disseminated by NSA analysts. Shea Decl. ¶¶ 20, 23.

The accessible results of an approved query are limited by the FISC's orders to records of communications within three "hops," or degrees of contact, from the seed. That is, the query results may only include identifiers and associated metadata having a direct contact with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop"

identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). *Id.* ¶¶ 22, 31. Query results do not include the names or addresses of individuals associated with the responsive telephone numbers, because that information is not included in the database in the first place. *Id.* ¶ 21.

The NSA's ability under this program to accumulate metadata in bulk, and to quickly conduct contact-chaining analyses beyond the first hop, is crucial to the utility of the database. These capabilities allow the NSA to conduct a level of historical analysis, and to discover contact links, that cannot practically be accomplished through targeted intelligence-gathering authorities. For example, the metadata may reveal that a seed telephone number has been in contact with a previously unknown U.S. number. Examining the chain of communications out to the second and in some cases a third hop may reveal a contact with other telephone numbers already known to be associated with a foreign terrorist organization, thus establishing that the previously unknown telephone number is itself likely associated with terrorism. This type of contact-chaining is possible because the bulk collection of telephony metadata under the program creates an historical repository that permits retrospective analysis of terrorist-related communications across multiple telecommunications networks, and that can be immediately accessed as new terrorist-associated identifiers come to light. *Id.* ¶¶ 46-49, 57-63; Skule Decl. ¶¶ 27-29.

Under the FISC's orders, the results of NSA's queries and analysis may be shared only to allow Government investigators to discover persons, including persons (and their associates) located in the United States, who have been in contact with known or suspected terrorist organizations, and may themselves be engaged in terrorist activity. The NSA does not use query results to provide the FBI with complete profiles even on suspected terrorists, or comprehensive records of their associations, without determining that they would be useful to the FBI's counter-terrorism mission. Nor does it indiscriminately provide the FBI with a list of all identifiers directly or indirectly connected (at one, two, and three hops) with a suspected terrorist identifier. Rather, NSA applies the tools of signals intelligence tradecraft to focus only on those identifiers which, based on its analytic judgment and experience, and other intelligence available to it, may be of use to the FBI in detecting persons in the United States who may be associated with the

specified foreign terrorist organizations, and acting in furtherance of their goals. Shea Decl. ¶¶ 26, 28; *see* Primary Order at 4.

In addition to these safeguards, the FISC's orders impose an extensive regime of internal reporting, audits, and oversight; regular consultation between the NSA Office of the Inspector General and the Department of Justice to assess compliance with FISC requirements; 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 query results containing U.S. person information have been shared with anyone outside NSA. Primary Order at 4-16.

III. Plaintiffs' Allegations

According to Plaintiffs' First Amended Complaint (ECF No. 9) ("FAC"),[2] Plaintiffs are social-welfare, interest-group, and political-advocacy organizations that bring suit on their own behalf and (purportedly) on behalf of their members, staff, and volunteers. FAC ¶¶ 2, 17-38, 40. Plaintiffs allege that in furtherance of their missions and operations, they make and receive telephone calls within the United States both to and from their members, staffs, constituents, and others. *Id.* ¶ 39. Based on the alleged premise that the NSA collects metadata on all (or at least the "vast majority") of the telephone calls transiting the networks of all major telecommunications carriers in the United States, *id.* ¶¶ 4-5, 53, 59, Plaintiffs assert that the NSA has acquired and retained call-detail records of their communications, *id.* ¶¶ 12, 60, 62. And although Plaintiffs' communications allegedly have no relevance to existing counter-terrorism investigations, *id.* ¶¶ 65, 72, Plaintiffs nevertheless assert that the NSA has searched and continues to search records of their telephone communications to construct "associational network graph[s]" of their communications patterns, thus "disclos[ing] the[ir] expressive and private associational connections," *id.* ¶¶ 7, 11-12, 69-71.

Plaintiffs allege that their associations and political-advocacy efforts (and those of their members and staffs) "are chilled by [this] search and analysis of information" about their

[2] 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. *OSU Student Alliance v. Ray*, 699 F.3d 1053, 1061 (9th Cir. 2012). 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.

telephone calls. *Id.* ¶ 64. Specifically, they assert in their complaint and in their motion papers that they "have lost the ability to assure their members and constituents [and others] that the fact of their communications to Plaintiffs will be kept confidential." *Id.* ¶¶ 63, 76; Pls.' Mem. at 20. As a result, Plaintiffs' members and constituents have allegedly become "very worried," "afraid," and "concerned" about the confidentiality of their communications with Plaintiffs, and "having their calls [with Plaintiffs] taped and stored" or "logged" by Government agencies. FAC ¶ 77; Pls.' Mem. at 22. Plaintiffs allegedly "ha[ve] experienced a decrease in communications from members and constituents" since the telephony metadata program became publicly known, FAC ¶ 76, and due to the "[k]knowledge" that their communications "may likely" be "monitored," have in some cases restricted what their employees and members say over the telephone about their organizational activities, or adopted other, more costly means of holding confidential conversations. *Id.* ¶ 77(d), (e); *see also* Pls.' Mem. at 21-23.

Plaintiffs maintain that the telephony metadata program thus violates their First, Fourth, and Fifth Amendments rights, and is not authorized under Section 215. FAC ¶¶ 80-105. By way of relief they seek an injunction "prohibiting [the Government's] continued use" of the program, an inventory of the records of their communications (assuming any) obtained under the program, and the destruction of those records remaining in the Government's possession. *Id.* at 24.

ARGUMENT

To avoid dismissal of their claims, Plaintiffs must show that their complaint "contain[s] sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation omitted). "[C]onclusory statements" and "bare assertions" of fact "are not entitled to the presumption of truth" and must be "discount[ed]" prior to "determining whether a claim is plausible." *Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1129 (9th Cir. 2013) (internal quotation omitted). A "claim has facial plausibility" when the remaining "well-pleaded allegations" allow "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678-79. Equally so, Plaintiffs cannot rely on "conclusory and bare bones" allegations to establish their standing to sue. *Perez v. Nidek Co.*, 711 F.3d 1109, 1113 (9th Cir. 2013).

The Court may grant Plaintiffs' summary judgment motion only if, when the evidence is viewed in the light most favorable to Defendants, there is no genuine issue as to any material fact and Plaintiffs are entitled to judgment as a matter of law. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986); *Anderson v. Liberty Lobby*, 477 U.S. 242, 255 (1986). Summary judgment must be denied if Plaintiffs fail to adduce sufficient evidence to establish an essential element of their claims, *Miller v. Glenn Miller Prods., Inc.*, 454 F.3d 975, 987 (9th Cir. 2006), such as their standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

I. PLAINTIFFS HAVE FAILED TO DEMONSTRATE 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). Demonstration of a plaintiff's standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan*, 504 U.S. at 560. The standing inquiry must be "especially rigorous" when reaching the merits of a claim would force the Court to decide whether actions of a coordinate Branch of the Federal Government in the field of intelligence gathering are unconstitutional. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013). To establish their standing, Plaintiffs must show they have suffered an injury in fact that is "concrete, particularized, and actual or imminent." *Id.* at 1147. Any "threatened injury must be *certainly* impending to constitute injury in fact," whereas "allegations of *possible* future injury are not sufficient." *Id.* The injury must be "fairly traceable to the challenged action" and be "redressable by a favorable ruling." *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752 (2010).

At the summary judgment stage, to show that they have standing Plaintiffs must submit "cognizable evidence of specific facts," and cannot rest on "mere allegations." *Snake River Farmers' Ass'n v. Dep't of Labor*, 9 F.3d 792, 795 (9th Cir. 1993); *see Lujan*, 504 U.S. at 561. The court may also consider extrinsic evidence on standing for purposes of resolving Defendants' Rule 12(b)(1) motion. *See Table Bluff Reserv. (Wiyot Tribe) v. Phillip Morris, Inc.*, 256 F.3d 879, 882 (9th Cir. 2001); *Augustine v. United States*, 704 F.2d 1074, 1077 (9th Cir.

1983). If Plaintiffs cannot carry their threshold jurisdictional burden of demonstrating their standing to sue, *Lujan*, 504 U.S. at 561, then "the [C]ourt cannot proceed" and must grant the Government's motion to dismiss, *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998), and deny Plaintiffs' partial summary judgment motion.

B. Plaintiffs Have Failed to Establish Their Standing

Plaintiffs' summary judgment motion should be denied, and the complaint dismissed, because Plaintiffs have failed to demonstrate an injury meeting Article III's standards. As discussed below, the consequences Plaintiffs are assertedly suffering as a result of the telephony metadata program arise from speculation on the part of their members, constituents, and others that the NSA has reviewed, or might in future review, call-detail records of their communications with Plaintiffs—and the consequent reluctance of these third parties to contact Plaintiffs for fear that the confidentiality of their communications may be compromised. These allegations are insufficient to confer standing on Plaintiffs, in particular because any resulting decisions by these third parties not to contact Plaintiffs are the product of their own unsubstantiated fears, and so are not fairly traceable to the telephony metadata program for Article III purposes.

Plaintiffs' core allegations of injury stem from their assertion that to carry out their organizational missions they engage in communications with members, constituents, and other persons who wish their communications with Plaintiffs to remain confidential. FAC ¶ 76; *see, e.g.*, HRW Decl. ¶¶ 4, 8, 10; CAIR-F Decl. ¶¶ 4, 6. Plaintiffs emphasize that these third parties allegedly contact them less frequently since the public revelation and media coverage of the telephony metadata program, *see, e.g.*, Bill of Rights Comm. Decl. ¶ 4; Shalom Center Decl. ¶ 7; Students Decl. ¶ 5; Franklin Armory Decl. ¶ 4; Calguns Decl. ¶ 6, PPR Decl. ¶¶ 6, 7; Acorn Decl. ¶ 7; NLG ¶ 4; CA-NORML Decl. ¶ 9; CAL-FFL Decl. ¶ 5; Media Alliance Decl. ¶ 9,[3] and that such third parties have expressed concern that their calls are being monitored, logged, or tracked by the NSA, or that they will be identified as supporting or being associated with a

[3] Besides the insufficiency of relating their asserted injury to the media's portrayal of the program, rather than the actual conduct of the program itself, *see Lujan*, 504 U.S. at 560 (injury must be fairly traceable to challenged conduct), the Ninth Circuit has held that assertions of "coincident" timing are, in the context of establishing a prima facie First Amendment violation, insufficient to demonstrate a "causal link" between the two events. *See Dole v. Local Union 375*, 921 F.2d 969, 971-73 (9th Cir. 1990) ("Documenting a result does not prove its cause.").

particular Plaintiff, *see, e.g.*, Acorn Decl. ¶ 8; Students Decl. ¶ 6; Bill of Rights Comm. Decl. ¶ 8b; Franklin Armory Decl. ¶ 4; UUSC Decl. ¶ 4; Free Software Decl. ¶¶ 4c, 5; Free Press Decl. ¶¶ 4, 5; CAL-FFL Decl. ¶ 4; Media Alliance Decl. ¶ 6; First Unitarian Decl. ¶¶ 4c, 8; CAIR-F Decl. ¶ 4d; CAIR-CA Decl. ¶ 11. *See also* FAC ¶ 77.

But these allegations are all based on speculative fears and misconceptions about the telephony metadata program, and are plainly insufficient to establish an injury satisfying the requirements of Article III. The fears of third parties that call-detail records collected by the NSA could be used to identify them as persons who associate with Plaintiffs are conjectural, at best, and arise in large part from a failure to grasp how the program operates. Thus, the resulting "chill" on their willingness to communicate with Plaintiffs cannot support Plaintiffs' standing. NSA personnel could identify persons with whom Plaintiffs speak by phone, either individually or collectively, only by retrieving and reviewing metadata records of calls to or from Plaintiffs (and then taking the next step of ascertaining the identities of the subscribers whose numbers are documented in the records). But under the FISC's orders, NSA 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; Shea Decl. ¶ 20. As a result, only a tiny fraction of the records are ever seen by any person. Shea Decl. ¶ 23. The complaint contains no well-pleaded, non-conclusory allegations, much less have Plaintiffs adduced any evidence, that records of their calls are among the very few that NSA has accessed or reviewed 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 NSA to develop "associational network graph[s]" of their contacts. FAC ¶ 7.

The Supreme Court's decision in *Amnesty International* establishes that such speculation concerning the reach of Government intelligence-gathering activities is insufficient to confer standing on Plaintiffs. In *Amnesty International*, various organizations challenged the constitutionality of amendments to FISA that 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 terrorism investigations, *see id.* at 1145-46, and that communications to which they were parties were likely therefore to be unlawfully intercepted. *Id.* at 1147. The Supreme Court held that this allegation of harm was insufficient to establish standing, because it was "speculative whether the Government w[ould] imminently target communications to which [the plaintiffs were] parties." *Id.* at 1148-50. The plaintiffs also argued, however, "that third parties might be disinclined to speak with them due to a fear of surveillance." *Id.* at 1152 n.7. The Court held that this assertion, even if factual, "d[id] not establish an injury that [was] fairly traceable" to the challenged statute, because it was "based on third parties' subjective fear of surveillance." *Id.* (citing *Laird v. Tatum*, 408 U.S. 1, 10-14 (1972)).

The same analysis is controlling here. Any concerns Plaintiffs may harbor about the confidentiality of their communications cannot give rise to standing, because it is just as speculative that records of their communications have been, or will be, reviewed under the telephony metadata program as it was in *Amnesty International* that "the Government w[ould] imminently target communications to which [the plaintiffs there] were parties." 133 S. Ct. at 1148. Any concerns of third parties about the confidentiality of their communications with Plaintiffs likewise "do not establish injury that is fairly traceable to" the telephony metadata program, "because they are based on third parties' subjective fear of surveillance," and not on the actual operation of the program. *See id.* at 1152 n.7; *see also Ass'n of Pub. Agency Customers v. Bonneville Power Admin.*, 733 F.3d 939, 950 (9th Cir. 2013) (injury cannot be "result of the independent action of some third-party not before the court") (internal quotations omitted), and not on the actual operation of the program.[4] Therefore, the subjective fears of

[4] In a similar vein, most Plaintiffs make the general assertion that now they can no longer assure their clients and other associates of the confidentiality of their communications, *see, e.g.*, Acorn Decl. ¶ 10, in other words, that they cannot allay the speculative fears of these third parties. This is no more than a repackaged version of their third-party "chill" argument, and suffers the same fate. *See Amnesty Int'l USA*, 133 S. Ct. at 1151 (refusing to accept a "repackaged version" of the plaintiffs' other "failed theory of standing").

these third-parties (and the concomitant effect on Plaintiffs) furnish insufficient grounds on which to base Plaintiffs' standing.[5]

The alternative and allegedly more costly and inefficient means of communicating that some Plaintiffs claim to have adopted to preserve the confidentiality of their contacts, such as holding in-person meetings, or communicating by U.S. mail,[6] "fare[] no better" as a basis on which to establish Plaintiffs' standing than the similar measures the plaintiffs took in *Amnesty International*, 133 S. Ct. at 1150-51.[7] This is so because Plaintiffs "do not face a threat of certainly impending" review under the "reasonable, articulable suspicion" standard of any records of their calls that may have been collected under the telephony metadata program. *See supra* at 12. Hence, "the costs that they have incurred to avoid" such scrutiny "are simply the product of their fear of surveillance," which the Supreme Court's decisions make clear "is insufficient to create standing." *Amnesty Int'l*, 133 S. Ct. at 1152; *Laird*, 408 U.S. at 10, 14 ("Allegations of a subjective 'chill'" arising from plaintiffs' knowledge of the existence of "a governmental investigative and data-gathering activity," without "any specific action of the [Government] against them," were "not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm"); *Vernon v. City of Los Angeles*, 27 F.3d 1385,

---

[5] Rendering these third parties' fears even more highly speculative is the fact that Plaintiffs have offered no proof that metadata of their calls actually have been or will imminently be collected under the telephony metadata program. The Government has acknowledged that the program remains ongoing, and that multiple electronic communication service providers have been participants in the program since its inception in 2006, *see supra* at 4-5, but it has not officially acknowledged the identities of the providers from which the Government continues to collect telephony metadata in bulk. Thus Plaintiffs can only speculate as to whether providers from which they receive telephone service have participated in the program—and this is insufficient. *See Amnesty Int'l USA*, 133 S. Ct. at 1147-48. The Government has acknowledged the authenticity of the now-expired April 25, 2013, FISC Secondary Order directed to Verizon Business Network Services (VBNS), but none of the Plaintiffs allege or provide evidence that they were VBNS customers during the lifespan of that order. Twenty-one of the twenty-four plaintiff organizations either do not identify the companies from which they obtain telephone service, or name companies other than VBNS. Three Plaintiffs attest that they are current customers of "Verizon Business," but do not specify whether they were customers of VBNS at the time the acknowledged April 25, 2013, Secondary Order remained in effect. Franklin Armory Decl. ¶ 6; Shalom Center Decl. ¶ 3; HRW Decl. ¶ 13.

[6] *See, e.g.*, Acorn Decl. ¶ 9; Charity & Security Network Decl. ¶¶ 5, 9; NLG Decl. ¶ 4; HRW Decl. ¶¶ 7, 9; PPR Decl. ¶ 12b; CAIR-F Decl. ¶¶ 4-5; CAIR-Ohio Decl. ¶¶ 9, 11, 15; PPR Decl. ¶ 12; Shalom Center Decl. ¶ 6.

[7] Many of these measures (such as delaying publishing articles or limiting content of telephone calls) seem to have nothing to do with the operation of the challenged program.

1394-95 (9th Cir. 1994) (applying *Laird* when plaintiff did not show actual monitoring of his First Amendment activities). To the extent Plaintiffs have adopted these alternative means of communication in an effort to allay the fears of their associates who may be reluctant to speak with Plaintiffs by telephone, then the injury is again traceable only to the subjective fears of these third parties, and not to the actual conduct of the telephony metadata program.[8]

In short, Plaintiffs' allegations of injury are plainly insufficient to establish Article III standing and avoid dismissal. In any event, they have failed to carry their burden of proving their standing in fact for purposes of summary judgment.

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

Even if Plaintiffs could demonstrate their standing, Congress has impliedly precluded judicial review of the type of statutory claim Plaintiffs assert—that is, a claim for declaratory and injunctive relief by telephone subscribers that the provision of telephony metadata to the Government, pursuant to a FISC order, violates Section 215. *See* FAC, ¶¶ 102-108. Thus, Plaintiffs cannot rely on the waiver of sovereign immunity codified in the Administrative Procedure Act (APA), 5 U.S.C. § 702, 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. *Id.* § 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,

[8] In *Vernon* the Ninth Circuit distinguished a prior case, *Presbyterian Church (USA) v. United States*, 870 F.2d 518 (9th Cir. 1989), in which the Court of Appeals had found *Laird* inapplicable. *See id.* at 521-23. In that case the Court of Appeals found standing existed where government agents actually "entered the churches wearing 'body bugs' and surreptitiously recorded church services," *id.* at 520, and, "as a result of the surveillance of worship services," *id.* at 521, those particular churches claimed injuries to their operations. *See id.* at 522. In contrast here, Plaintiffs have not properly alleged or adduced evidence that any of the telephony metadata associated with their calls (never mind the content of those calls) has been, or certainly will be, reviewed or analyzed by the NSA.

sovereign immunity shields the Federal Government and its agencies from suit."). It is further axiomatic that the existence of consent to sue the United States "is a prerequisite for jurisdiction." *United States v. Mitchell*, 463 U.S. 206, 212 (1983). 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." *Id.* § 701(a)(1) ("This chapter applies, according to the provisions thereof, except to the extent that 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.

The USA PATRIOT Act permits specified suits against the United States but impliedly forbids Plaintiffs' statutory claim for equitable relief. Two provisions of that Act are pertinent. First, section 223 of the Act, 18 U.S.C. § 2712, titled "Civil actions against the United States," authorizes suits against the United States to recover money damages only—not injunctive relief—for willful violations of the Wiretap Act, the Stored Communications Act (SCA), and three particular provisions of FISA, all involving the use and disclosure of information, not its collection. Pub. L. No. 107-56, § 223, 115 Stat. 294 (2001). 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 (and even if they were, it would only be for money damages, not injunctive relief).[9] 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.

This Court recently reached this very conclusion in the *Jewel* and *Shubert* cases, a broader challenge to alleged NSA "dragnet" acquisition of communications records and

[9] 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.

surveillance of communications content after the 9/11 attacks. *Jewel v. NSA*, 2013 WL 3829405 (N.D. Cal. July 23, 2013). The Court concluded there that § 2712, "by allowing suits against the United States only for damages based on three provisions of [FISA], impliedly bans suits against the United States that seek injunctive relief under any provision of FISA." *Id.* at *12. Thus, the Court held that the plaintiffs 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 here.[10]

Second, Section 215 forecloses the specific statutory claim for injunctive relief asserted here, by this type of plaintiff, in this forum. 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)(1), (f)(2)(A)(i), (B). Congress explicitly stated that the FISC petition review pool "shall have jurisdiction to review petitions filed pursuant to section 1861(f)(1) . . . of this title." *Id*. § 1803(e)(1). Congress provided for further review of the resulting FISC's decisions in the FISA Court of Review and the Supreme Court, not in district court. *Id*. § 1861(f)(3). Congress also expressly provided that a Section 215 order "shall remain in effect" unless it has been "explicitly modified or set aside consistent with this subsection." *Id.* § 1861(f)(2)(D). Thus, Congress specifically authorized challenges to Section 215 production orders only by recipients of those orders—the entities that create and own the records, *see United States v. Miller*, 425 U.S. 435, 440-41 (1976)—and permitted those entities to challenge production orders only by filing a challenge in the FISC, thereby impliedly precluding a challenge brought by subscribers of telecommunications services in district court.

Congress chose this process for subjecting Section 215 orders to "a substantial and engaging adversarial process," Aug. 29 FISC Op. at 15, in order to ensure meaningful judicial review of those orders while at the same time protecting the critical national security interests that FISA is designed to advance. The purpose of Section 215's judicial review procedure was to "place Section 215 proceedings on a par with grand jury proceedings, where the subpoena

[10] The *Jewel* plaintiffs' FISA claim, brought under 50 U.S.C. §§ 1809, 1810 (*see Jewel*, 2013 WL 3829405 at *3), was also not included in the list of FISA claims actionable under § 2712, as is the case here. *See id*. at *12 (noting the plaintiffs' argument that they were bringing a different claim, seeking different relief, from the specific FISA provisions listed in § 2712(a)).

recipient obviously knows of its existence and can challenge it in court." *Implementation of the USA PATRIOT Act: Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary*, 109th Cong. at 65 (2005) (statement of Robert Khuzami). Congress specifically considered whether to extend a similar right of action to third parties but declined to do so because it would have been incompatible with the secrecy required for Section 215 orders.[11] To promote its effective functioning as a tool for counter-terrorism, Section 215, like other provisions of FISA, establishes a secret and expeditious process that involves only the Government and the recipient of the order. *See* 50 U.S.C. § 1861(d)(1) (recipient may not "disclose to any other person that the [FBI] has sought or obtained" a production order). Under the statutory framework, third parties such as Plaintiffs, who are not recipients of Section 215 orders, are not even supposed to know of their existence, nor play a role in the process of testing their compliance with the statute. *See, e.g.*, H.R. Rep. No. 109-174 at 128 (2005). The fact that Plaintiffs learned about the program they seek to challenge as the result of an unauthorized and unlawful disclosure does not change this essential facet of FISA's structure. Allowing third parties to contest an order's compliance with Section 215's relevance and other requirements would potentially compromise the secrecy and efficiency of the process Congress envisioned.

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 market orders precluded suits by consumers); *Overton Power District No. 5 v. O'Leary*, 73 F.3d 253, 256 (9th Cir. 1996) (power suppliers lacked right of action to challenge rate-setting decision where Congress intended only contractors named in statute to do so); *Dellums v. Smith*, 797 F.2d 817, 823 (9th Cir. 1986) (private citizens lacked right of action to challenge Attorney General's decision not to conduct preliminary investigation under the Ethics in Government Act, where Congress envisioned

[11] *See id*. ("Beyond this amendment, however, the confidentiality provisions of Section 215 should not be disturbed. You do not want potential terrorists to know you are investigating them or are aware of their plans."). *See also* H.R. Rep. No. 109-174 at 128 (right to challenge Section 215 order can only be given to the recipient, not the target, because the target does not know about it); *id.* at 268 (statutory prohibition on disclosing Section 215 order to subject prevents the subject from challenging it).

enforcement by congressional judiciary committees, not private citizens); *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 Stored Communications Act 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).

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

Plaintiffs assert that NSA's collection of bulk telephony metadata is not authorized under Section 215 because (i) the records obtained are not "relevant" to authorized national security investigations, (ii) the Stored Communications Act, 18 U.S.C. § 2701, *et seq.* (SCA), does not permit the Government to obtain telephony metadata pursuant to Section 215; and (iii) Section 215 does not authorize the FISC to order production of electronic business records on a prospective basis. Pls.' Mem. at 6-17. Even if review of Plaintiffs' statutory claim were not precluded, these contentions lack merit and should be rejected.

A. The Government's Bulk Collection of Telephony Metadata Comports With Section 215's Relevance Requirement.

Section 215 authorizes the FISC to order "production of any tangible things" upon application by the FBI "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [counter-terrorism] investigation." 50 U.S.C. § 1861(a)(1), (b)(2)(A). Since May 2006, fifteen separate judges of the FISC have concluded on thirty-five occasions that the Government satisfied this requirement. Skule Decl. ¶¶ 6, 11. Plaintiffs now ask this Court to second-guess the FISC's repeated conclusions and declare instead that the call-detail records the FISC ordered produced to the NSA are not, in fact, relevant to authorized counter-terrorism investigations. The Court should reject this invitation.

1. The bulk telephony metadata collected under the FISC's orders are "relevant" to authorized national security investigations.

The concept of "relevance" has developed an accepted 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 must be enforced 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). 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, *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984).

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.[12] Analogously, courts also issue search warrants permitting Government agents to copy entire computer hard drives and then later review their contents for the specific evidence described in the warrant. *See* Fed. R. Crim. P. 41(e)(2)(B).[13]

Both the text and legislative history confirm that Congress was acutely aware of and incorporated this accepted legal concept of relevance when it enacted Section 215's relevance

[12] *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 investigation); *Goshawk Dedicated Ltd. v. American 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").

[13] *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).

requirement, *see* USA PATRIOT Act Improvement Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2006). It was well recognized at the time that relevance was the equivalent of the "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).[14] And Congress in fact 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).[15]

Of course, the case law in these contexts does not involve data acquisition on the scale of the telephony metadata collection authorized by the FISC, because the information gathered in these contexts is sought in aid of focused judicial and administrative proceedings involving identifiable individuals and events. But in this context relevance must be evaluated in light of the special nature, purpose, and scope of national security investigations. *See Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946). Routine criminal or administrative inquiries, which ordinarily focus retrospectively on specific crimes or violations that have already occurred and the persons known or suspected to have committed them. The key purpose of counter-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"); *United*

[14] *See also* 152 Cong. Rec. S1379, 1395 (Feb. 16, 2006) (statement of Sen. Kyl) ("We all know the term 'relevance' . . . . 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); H.R. Rep. No. 109-174, pt. 1 at 131 (statement of Rep. Lungren).

[15] *See also 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 to incorporate the established meaning of these terms.").

States v. U.S. Dist. Court (Keith), 407 U.S. 297, 322-23 (1972); Skule Decl. ¶¶ 17-18. Relevance in this context, therefore, must take into account the far-reaching information-gathering required 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 ("[M]any 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). Consistent with this core legislative objective, Section 215 should be understood to authorize the collection of records that can help to identify previously unknown operatives and activities, and thus detect and prevent terrorist attacks before they are launched.

Bulk telephony metadata are therefore relevant (at the least) to FBI counter-terrorism investigations because, as experience has shown, the collection and aggregation of these data permit the effective use of NSA analytical tools to detect contacts between foreign terrorists and their unknown associates located in the United States who may be planning attacks on the U.S. soil. Skule Decl. ¶¶ 8-9, 18-26; Shea Decl. ¶¶ 44, 46-48; *see* Aug. 29 FISC Op. at 20. Targeted tools of investigation that do not involve bulk collection of the data cannot always achieve this objective as effectively, if at all, because the Government cannot know, in advance of linking a phone number (or other identifier) to a terrorist organization, where in the data the terrorists'

communications can be found. Skule Decl. ¶¶ 9, 27-29; Shea Decl. ¶¶ 57-63. Absent the creation of an historical repository of information that bulk collection and aggregation of the data allow, it may not be feasible for NSA to identify chains of communications among known and unknown terrorist operatives that cross different time periods and providers' networks. Skule Decl. ¶¶ 9, 27-29; Shea Decl. ¶ 60; *see* Aug. 29 FISC Op. at 21-22. Thus, there are reasonable grounds, at the least, for concluding that "the whole of the metadata produced" is "relevant" to authorized national security investigations. Aug. 29 FISC Op. at 22.[16]

2. Congress has legislatively ratified the construction of Section 215 as allowing for the bulk collection of telephony metadata records

The conclusion that bulk telephony metadata are "relevant" within the meaning of Section 215 is reinforced, as the FISC recently recognized, by Congress's extension of Section 215's authorization in 2010 and 2011, without substantive change, after receiving notice that the FISC and the Executive Branch had interpreted Section 215 to authorize the bulk collection of telephony metadata. Aug. 29 FISC Op. at 23-28. On both occasions 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."[17] Additionally, the classified use of this authority has been

[16] Notably in this regard, Section 215 permits the collection of information relevant "to an authorized investigation," 50 U.S.C. § 1861(b)(2)(A), not simply information relevant to the "subject matter" involved, as in civil discovery, Fed. R. Civ. P. 26(b)(1). Business records can therefore be "relevant" to an investigation not merely if they relate to its subject matter, but also if there is reason to believe they are necessary or useful to the application of investigative techniques that will advance its purposes. As discussed above, NSA analysis enables 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.

[17] *See* Letter from Ronald Weich to the Hon. Silvestre Reyes (Dec. 14, 2009) (Exh. G); Report on the [NSA's] Bulk collection Programs for USA-PATRIOT Act Reauthorization (Exh. H). 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. I); Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (Exh. J); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep.

briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees, as several Members of Congress have acknowledged.[18]

After receiving these "extensive and detailed" briefing papers "regarding the nature and scope" of the program, Congress twice extended Section 215's authorization, in 2010 and 2011. Aug. 29 FISC Op. at 25 & n.23.[19] "'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. Imposing a limiting construction now on Section 215 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.[20]

Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden). An updated version of the briefing paper, *see* Exh. M, 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. K); Letter from Ronald Weich to the Hon. Mike Rogers and the Hon. C.A. Dutch Ruppersberger (Feb. 2, 2011) (Exh. L). 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) (Exh. N).

[18] *See* Press Release of Sen. Select Comm. on Intelligence (June 6, 2013) (Exh. O)); *How Disclosed NSA Programs 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. P).

[19] 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.

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).

[20] Plaintiffs overstate the requirements for application of the doctrine of legislative ratification. Pls.' Mem. at 15-17. The Supreme Court has often found "clear[ ]" and "undoubted" Congressional awareness of the pertinent judicial and executive interpretations based on references in committee reports, without requiring evidence as to how many Members of Congress actually read those reports. *See EEOC v. Shell Oil Co.*, 466 U.S. 54, 69 & n.21 (1984); *Haig v. Agee*, 453 U.S. 280, 297-98 & n.37 (1981); *NLRB v. Gullett Gin Co.*, 340 U.S. 361, 365-66 & n.3 (1951).

3. Plaintiffs present no persuasive reasons for second-guessing the FISC's repeated conclusions that bulk telephony metadata are "relevant" to authorized counter-terrorism investigations

Plaintiffs nevertheless maintain that the NSA's FISC-authorized collection of bulk telephony metadata exceeds the Government's authority under Section 215 because it disregards the relevance requirement. But since May 2006, fifteen separate judges of the FISC have concluded otherwise, finding "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." Skule Decl. ¶¶ 6, 11; *see* Primary Order at 1; Aug. 29 FISC Op. at 11; Oct. 11 FISC Mem. at 3.[21] As the FISC concluded recently:

> [b]ecause known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, the production of the information sought meets the standard for relevance under Section 215.

Aug. 29 FISC Op. at 18; *see also* Oct. 11 FISC Mem. at 3.

Considering that the Government has consistently demonstrated the relevance of the requested records to the FISC's satisfaction, as Section 215 requires, it is difficult to understand how the Government can be said to have acted in excess of its statutory authority. At bottom, Plaintiffs are asking this Court to conclude that the FISC exceeded *its* authority when it authorized the NSA's bulk collection of telephony metadata, and that this Court should substitute its judgment for the decisions that the FISC reached thirty-five times.

That approach cannot be reconciled with the legislative plan. When courts are called on to enforce grand jury or administrative subpoenas—instruments that informed Congress's understanding of Section 215, *see supra* at 19 & n.11—the Government's determination that records are "relevant" to its investigation is subject only to the most deferential review.[22] In the

[21] In another recently released FISC opinion, the FISC concluded that bulk collection of Internet metadata satisfied the relevance requirement of FISA's pen/trap provision, 50 U.S.C. § 1842, because bulk collection of the metadata was necessary for the NSA to employ analytical techniques that generate useful leads for FBI counter-terrorism investigations. *[Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order (F.I.S.C. [redacted]) (declassified and released on Nov. 18, 2013) (Exh. Q) ("*[Redacted]*") 47-49; *see id.* at 40-46.

[22] *See R. Enters.*, 498 U.S. at 301 (grand jury subpoena challenged on relevancy grounds must be upheld 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

analogous context of electronic surveillance, FISC orders receive only "minimal scrutiny by [reviewing] courts." *United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010).

An equally deferential standard of review is called for in this context, where ensuring the Government's access to the information needed to carry out its national security mission is imperative, and where deferential review is commanded by the terms of Section 215 itself. Section 215 conditions the Government's access to business records, not on a showing of relevance, but on a showing of "*reasonable grounds to believe* that the [records] are relevant" to authorized counter-terrorism investigations. 50 U.S.C. § 1861(b)(2)(A) (emphasis added), (c)(1). Under this standard, in order to find that the FISC's production orders exceeded its authority, this Court would have to conclude that the fifteen FISC judges who repeatedly issued those orders lacked any reasonable basis for doing so. That proposition is self-defeating.

Principally, Plaintiffs argue that bulk telephony metadata cannot be considered relevant under Section 215 because the vast majority of the records collected are not related to specific counter-terrorism investigations. Pls.' Mem. at 7-8. But the Government has always acknowledged, and the FISC has understood, that the vast majority of the call-detail records the Government expects to collect do not themselves document communications between terrorist operatives. *See supra* at 6; Shea Decl. ¶¶ 5, 23-24; Aug. 29 FISC Op. at 20-23. At the same time, the FISC has recognized that bulk collection of the data is necessary to the program—and therefore that the records are relevant as a whole—because the NSA cannot know in advance of making authorized queries (under the "reasonable articulable suspicion" standard) which communications occurring at what times, on which providers' networks, will reflect connections between terrorist groups and operatives located in the United States. *See id.* at 22. Thus, the collateral acquisition of records that do not pertain to such communications is not evidence that the Government (or the FISC) has exceeded its authority, but an outgrowth of the leeway that Congress extended to the Government—subject to statutory and court-ordered safeguards—to

---

investigation"); *NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006) (in a proceeding to enforce an administrative subpoena, the agency's appraisal of relevancy to its investigation "must be accepted so long as it is not obviously wrong," and the district court's finding of relevancy will be affirmed unless it is "clearly erroneous"); *FTC v. Invention Submission Group*, 965 F.2d 1086, 1089 (D.C. Cir. 1992) (same).

obtain foreign intelligence information under Section 215 "to meet its national security responsibilities." *Id.* at 11, 23; *see* Shea Decl. ¶¶ 29-35.[23]

Plaintiffs invoke the principle that "[g]rand juries are not licensed to engage in arbitrary fishing expeditions." *R. Enters.*, 498 U.S. at 299. But the FISC's decisions authorizing the NSA's bulk collection of telephony metadata cannot be dismissed as arbitrarily licensing "fishing expeditions into private papers . . . in the [mere] hope that something will turn up." Pls.' Mem. at 7 (citing *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 305-06 (1924)). Rather, as the FISC has stated, prior experience "demonstrate[es] that information concerning known and unknown affiliates of international terrorist organizations [is] contained within the non-content metadata the government [seeks] to obtain." Aug. 29 FISC Op. at 20; *see also id.* at 21 ("'[a]nalysts know that the terrorists' communications are located somewhere' in the metadata"); Shea Decl. ¶¶ 52-55. Reason and experience also teach that the data are relevant, and fruitful, to the FBI's core mission of protecting national security. The NSA's analysis of bulk telephony metadata produces valuable tips and leads that have given rise (or new impetus) to FBI counter-terrorism investigations, and contributed to the prevention of terrorist attacks. *Id.* ¶¶ *44-56;* Skule Decl. ¶¶ 18, 20-26. Plaintiffs disclaim knowledge "of any precedent" that supports a finding of relevance on these grounds, Pls.' Mem. at 9, but in the counter-terrorism context at issue here, the FISC has upheld the bulk collection of telephony metadata on this basis thirty-five times.

The reasoning adopted by the FISC does not render the limits of relevance "illusory," as Plaintiffs predict. Pls.' Mem. at 9. The relevance of bulk telephony metadata is a function of

[23] Notably, when Congress passed the USA PATRIOT Act in 2001, it expanded the Government's authority to obtain business records under FISA by eliminating the requirement in prior law of "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." 50 U.S.C. § 1862(b)(2)(B) (2000 ed.); Pub. L. 107-56, § 215, 115 Stat. 288; *see* Aug. 29 FISC Op. at 13. Again in 2006, when Congress codified Section 215's relevance requirement, it rejected a proposal to restrict the statute's scope to records pertaining to individuals suspected of terrorist activity. *See* S. 2369, 109th Cong. § 3, *reprinted at* 152 Cong. Rec. S1791 (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, [to] suspected . . . 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). 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, not vindicate, the will of Congress.

distinctive characteristics not common to most other types of records—specifically, their highly standardized and inter-connected nature, which makes them easily susceptible of analysis in large datasets to bring previously unknown connections with suspected terrorist operatives to light, Shea Decl. ¶ 46, and enable the Government to identify individuals who may be planning terrorist attacks against this Nation. Precisely because the concept of relevance is so inherently "variable in relation to the nature, purposes, and scope of [an] inquiry," *Oklahoma Press*, 327 U.S. at 209, a decision here that bulk telephony metadata are relevant, as a whole, to counter-terrorism investigations in no way foretells, much less compels, the decision the FISC would reach were the Government to seek an order directing bulk production of other records. The result in any such case would depend, at the least, on the nature of the records in question, the bearing they have on the Government's investigations, the scope of the production sought, and any constitutional considerations, none of which can be predicted or assessed in the abstract.[24]

In the final analysis, Plaintiffs succeed only in proving their own disagreement with the FISC's repeated determinations that bulk telephony metadata are relevant to FBI counter-terrorism investigations. They cite nothing in the text or legislative history of Section 215 demonstrating that the FISC, in reaching those conclusions, exceeded the authority that Congress intended it to exercise. Congress assigned the FISC the responsibility of making relevance determinations under Section 215, and Plaintiffs have not explained how the FISC has exercised that authority in a way, not simply that they object to, but that Congress did not intend.[25]

---

[24] Observing that Section 215 permits the acquisition of "such thing[s] [as] can be obtained with a [grand jury] subpoena duces tecum," 50 U.S.C. § 1861(c)(2)(D), Plaintiffs argue at length that the Government has exceeded its authority because bulk collection of telephony metadata exceeds the scope of production that a grand jury could obtain by subpoena. Pls.' Mem. at 9-11. As an initial matter, subparagraph (c)(2)(D) concerns the type, not the volume, of records the Government may obtain pursuant to a Section 215 order. Moreover, in support of their argument Plaintiffs cite a series of cases (all but one long preceding the Supreme Court's decision in *R. Enterprises*) holding that grand jury subpoenas "seeking the entirety of a person's documents are improper." *Id.* (citing, *inter alia*, *Hale v Henkel*, 201 U.S. 43, 76 (1906), *and Schwimmer v. United States*, 232 F.2d 855, 8611 (8th Cir. 1956)). These cases are not instructive for purposes here, because the bulk collection of telephony metadata does not involve the compelled production "of the entirety of [anyone's] documents," particularly Plaintiffs'. Rather, it involves a single, specified class of records—call-detail records—that are created and maintained by, and belong to, telecommunications service providers.

[25] Two groups of *amici* argue in support of Plaintiffs, respectively, that they "have seen" no evidence that the telephony metadata program has "provided any intelligence of value that could not have been gathered through less intrusive means," Brief of *Amici Curiae* Senator[s]

B. The Stored Communications Act Does Not Prohibit the Government's Acquisition of Telephony Metadata Pursuant to Section 215.

Plaintiffs next argue that the Government's collection of call-detail records under Section 215—whether in bulk or otherwise—is prohibited by the SCA, specifically, 18 U.S.C. § 2703(c). The FISC has previously held otherwise, *In re Prod. of Tangible Things from [Redacted]*, Dkt. No. BR 08-13, Supp. Op. (F.I.S.C. Dec. 12, 2008) (Exh. R), and so, too, should this Court.

Section 2703, enacted by § 201(a) of the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 ("ECPA") (Title II of which is known as the SCA), provides that a governmental entity may require providers of electronic communication or remote computing service to disclose records or other information pertaining to their subscribers or customers (other than the contents of communications) only when one of five conditions is met, 18 U.S.C. § 2703(c)(1)(A)-(E), including circumstances when, as pertinent here, the government "obtains a court order for such disclosure under subsection (d)." *Id.* § 2703(c)(1)(B). Subsection 2703(d) provides that a court may issue an order for disclosure of communications records under subsection (c) on a showing by the government "of specific and articulable facts showing that there are reasonable grounds to believe that the … records or other information sought … are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

Because disclosure pursuant to Section 215 for purposes of a counter-terrorism investigation is not among the five enumerated circumstances under which subsection 2703(c) authorizes the Government to obtain communications records from a provider, Plaintiffs contend that production of telephony metadata under Section 215 is barred by the SCA. Pls.' Mem. at 12. But Plaintiffs overlook subsection (c) of Section 215 itself, 18 U.S.C. § 1861(c). When the FISC finds "that the [Government's] application meets the requirements" for a production order, *id.* § 1861(c)(1), Section 215 provides that the Government may acquire "such thing[s] [as] can

---

Wyden, *et. al.*, at 2, and that the Court should "apply Section 215's 'relevance' requirement as a restraint on expansive surveillance . . . ." Brief *Amicus Curiae* of Experts in the History of Executive Surveillance at 15. So long as the telephony metadata program is lawful—and it is—any question as to whether the program should continue in its present form is a matter of national security for the political branches, not the courts, to decide. *See Dep't of the Navy v. Egan*, 484 U.S. 518, 530 (1988). It is a question to which Congress even now is devoting substantial attention, and one that Congress will have to decide, one way or another, before Section 215's current authorization expires on June 1, 2015. *See* Pub. L. 109-177 § 102(b)(1), 120 Stat. 195 (50 U.S.C. § 1805 note), as amended by Pub. L. 112-4 § 2(a), 125 Stat. 216.

be obtained with a [grand jury] subpoena . . . *or with any other order issued by a court of the United States directing the production of records or tangible things.*" *Id.* § 1861(c)(2)(D) (emphasis added). Subsections 2703(c) and (d) of the SCA make clear that subscriber communications records may be obtained by the Government pursuant to an order issued by a U.S. court directing their production. Hence, by operation of the express terms of 50 U.S.C. § 1861(c)(2)(D), the same records may also be obtained under authority of Section 215. *See In re Prod. of Tangible Things, supra*, Supp. Op. at 2 n.1. As the FISC observed, this result also promotes the objective of a coherent and harmonious legislative scheme. *Id.* at 4-5.

C. Nothing in Section 215 Prohibits the FISC from Prospectively Directing the Production of Electronic Business Records as They Are Created

Finally, Plaintiffs make a two-fold argument that Section 215 does not permit the FISC to order the production of electronic business records of any kind, or to do so on a prospective basis, because such records do not constitute "tangible things" within the meaning of the statute. Pls.' Mem. at 13-15. Congress passed the USA-PATRIOT Act, including Section 215, to provide the Government with 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(1) at 4. Yet Plaintiffs posit that in the immediate wake of the September 11, 2001, attacks, in the full bloom of the digital age, Congress intended to relegate this important tool for combatting terrorism to the acquisition of paper records. That untenable proposition should be rejected.

Section 215 authorizes the FISC to order "production of tangible things (including books, records, papers, documents, and other items) . . . ." 50 U.S.C. § 1861(a)(1). The meaning of the word "tangible," as understood at the time the statute was enacted, *see BedRoc, Ltd. v. United States*, 541 U.S. 176, 184 (2004); *cf.* Pls.' Mem. at 14 & n.6, is "able to be perceived as materially existent, especially by the sense of touch," or "substantially real" or "material." Webster's Third New Int'l Dictionary (2002); *see also* The American Heritage Dictionary (4th ed. 2000) (defining "tangible" as "possible to be treated as fact, real or concrete"). Thus, the term "tangible" can be used to connote not only tactile items such as pieces of paper, but other things that are perceptible as materially existent or real, such as electronically stored information.

Any question about the matter is resolved by the statute's inclusion of "documents" and "records" among the "tangible things" whose production can be compelled. These terms have been understood for decades to include electronically stored information. For example, as long ago as 1970, the description of the term "documents" in Rule 34 of the Federal Rules of Civil Procedure was amended to include "data compilations," in order "to accord with changing technology" and "make clear that Rule 34 applies to electronic data compilations from which information can be obtained . . . ." *Proposed Amendments to the Fed. R. Civ. P. Relating to Discovery*, 48 F.R.D. 487, 525, 527 (1970). That understanding had entered common usage by the time Section 215 was enacted. *See* The American Heritage Dictionary (4th ed. 2000) (defining "document" to include "a computer file contain[ing] …data").

Plaintiffs' related contention, that Section 215 does not authorize the FISC to compel production of records "on an ongoing daily basis . . . for the duration of [its] [o]rder[s]," Secondary Order at 2, because the records "do not yet exist" at the time an order is issued, Pls.' Mem. at 13, is equally meritless. Nothing in the statute's terms suggests that FISC orders may apply only to records created before an order is rendered. What is pertinent under the statute is that the records exist at the time of production, and that nothing in the FISC's orders require the creation of records that providers otherwise would not keep. Notably, courts have held that the Government may seek prospective disclosure of communications 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).[26] The same is true under Section 215.

[26] *See also United States v. Booker*, 2013 WL 2903562, *6-7 (N.D. Ga. June 13, 2013); *In re Application of the United States*, 622 F. Supp. 2d 411, 418-19 (S.D. Tex. 2007); *In re Application of the United States*, 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006); *In re Application of the United States*, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006); *In re Application of the United States*, 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re Application of the United States*, 405 F. Supp. 2d 435, 446-47 (S.D.N.Y. 2005).

IV. THE TELEPHONY METADATA PROGRAM DOES NOT VIOLATE PLAINTIFFS' FOURTH AMENDMENT RIGHTS.

Even assuming, *arguendo*, that Plaintiffs had established their standing, their remaining claims under the First, Fourth, and Fifth Amendments should still be dismissed, and their motion for summary judgment on their First Amendment claim denied, because the telephony metadata program adheres to all constitutional requirements.

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 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 pursuant to orders of the FISC does not involve a "search" of individual subscribers or their property, ending the Fourth Amendment inquiry. 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*, 442 U.S. 735, 741-46 (1979), 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. In contrast to the contents of telephone calls, the Court doubted that individuals had any actual expectation of privacy in telephone numbers they 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. The third-party doctrine has consistently been applied to telephone call detail records like the business records at issue here, which are also third-party records. *See, e.g., Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1043-46 (D.C. Cir. 1978); *United States v. Baxter*, 492 F.2d 150, 167 (9th Cir. 1973); *United States v. Fithian*, 452 F.2d 505, 506 (9th Cir. 1971). In recent years the Ninth Circuit has also applied *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), and 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).

Smith is fatal to Plaintiffs' claim that the collection of their telephony metadata violates the Fourth Amendment. *See United States v. Moalin*, 2013 WL 6079518, *6-8 (S.D. Cal. Nov. 18, 2013) (relying on *Smith* to reject criminal defendant's argument that NSA's collection of metadata about his telephone calls, which were then used to link him to a Somali terrorist group, violated his Fourth Amendment rights); Aug. 29 FISC Op. at 6 ("The production of telephone service provider metadata is squarely controlled by *Smith* . . . . [*Smith*] and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years."); *cf. [Redacted]*, Opinion & Order at 58-66 (bulk collection of Internet metadata does not violate the Fourth Amendment). So far as metadata include such information as the times and duration of calls, and the dialing and receiving numbers, that is

information that telephone subscribers voluntarily turn 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; FAC ¶ 54. 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 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.

Importantly, the call-detail records reveal only phone numbers and other routing information, not the names or addresses of the parties to the calls. *See* Shea decl. ¶¶ 15, 21; Skule Decl. ¶¶ 7, 11. Thus, these data do not in fact reveal any information about the subscriber's associations or activities. The mere fact that the numbers dialed from a phone could, in some hypothetical sense, reveal the identities of the persons and the places called, was raised by the dissenters in *Smith*, 442 U.S. at 748 (Stewart, J., dissenting), where, unlike here, the government did know the caller's identity, but the Court nonetheless ruled that there is no reasonable expectation of privacy in telephone numbers dialed. *Id*. at 741-42.

Smith is not distinguishable on the basis of the broad scope of the telephony metadata program. *See [Redacted]*, Opinion & Order at 62-63. 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,Minnesota v. Carter*, 525 U.S. 83, 88 (1998); *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978). No Fourth Amendment interest of Plaintiffs is implicated, therefore, by virtue of the fact that the metadata 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).

Thus, *Smith* controls the outcome here. There has been no "search" of metadata about Plaintiffs' telephone calls, for purposes of the Fourth Amendment.

B. The Government's Acquisition of Telephony Metadata Is Reasonable

Even if collecting telephony metadata involved a Fourth Amendment "search," 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. As the Supreme Court has explained, "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665-66 (1989). More specifically, the scope of the legitimate expectation of privacy and the character of the intrusion are balanced against the nature of the government interests to be furthered, as well as the immediacy of the government's concerns regarding those interests and the efficacy of the policy at issue in addressing those concerns. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 658, 660, 662-63 (1995).

The NSA's collection of telephony metadata clearly serves special governmental needs above and beyond normal law enforcement. The undisputed programmatic purpose of the collection of this metadata is identifying unknown terrorist operatives and preventing terrorist attacks—forward-looking goals that fundamentally differ from most ordinary criminal law enforcement, which typically focuses on solving crimes that have already occurred, not preventing unlawful activity and protecting public safety and national security. *See, e.g., Keith*, 407 U.S. at 322-23; *In re Sealed Case*, 310 F.3d 717, 746 (FISC-R 2002).

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 written into the FISC's orders. Primary Order, at 4-14. *See also Maryland v. King*, 133 S. Ct. 1958, 1979 (2013); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 833 (2002); *Vernonia*, 515 U.S. at 658.

On the other side of the balance, the collection and analysis of telephony metadata promote 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 v. Agee*, 453 U.S. 280, 307 (1981) ("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."). Requiring individualized suspicion here would indeed be impracticable. The Government's interests in identifying unknown terrorist operatives and preventing terrorist attacks cannot be as effectively achieved by requiring individualized suspicion to collect metadata, because such a requirement would not permit the type of historical analysis and contact chaining that the broader collection enables and to quickly identify contacts. *See* Aug. 29 FISC Op. at 20-22. Given that the program might be rendered entirely infeasible, it would certainly be "impracticable" to require individualized suspicion in this context. *See Von Raab*, 489 U.S. at 665-66.

V. PLAINTIFFS' FIRST AMENDMENT CLAIM FAILS AS A MATTER OF LAW

A. Good-Faith Investigatory Conduct Not Intended to Deter or Punish Protected Speech or Association Does Not Violate the First Amendment

Plaintiffs' First Amendment claim, that the FISC-authorized collection of telephony metadata violates their expressive and associational rights, FAC ¶¶ 78-83, Pls.' Mem. at 17-25, perishes in the wake of their failed Fourth Amendment claim. Recognizing the need to accommodate the Government's interests where prevention of crime, or, even more imperatively, potential threats to national security are concerned, 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, or compulsory nature that is directed against individuals based on their expressive or associational activities. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Laird*, 408 U.S. at 11; *United States v. Mayer*, 503 F.3d 740, 751-53 (9th Cir. 2007). Accordingly, the law is clear that governmental investigative activities conducted in good faith—that is, not "for the purpose of abridging first amendment freedoms"—do not violate the First Amendment. *Mayer*, 503 F.3d at 751. *See also Reporters Comm.*, 593 F.2d at 1051-53.

Here, Plaintiffs do not contend that the Government's collection of non-content telephony metadata has any objective other than furthering the compelling national interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks. Neither their complaint nor their declarations even purport to assert that such collection is aimed at curtailing any First Amendment expressive or associational activities. *See Mayer*, 503 F.3d at 752. To the contrary, Plaintiffs' allegations regarding the FISC-authorized breadth of the collection, FAC ¶¶ 4-6, 11, 53-55, 59-60; Pls.' Mem. at 1-5, 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.

B. The Telephony Metadata Collection Program Imposes No Direct or Significant Burden on Plaintiffs' Speech or Associational Rights

Plaintiffs' contention that the challenged program should be subjected to "exacting scrutiny" because it burdens Plaintiffs' associational rights, Pls.' Mem. at 18-24, also fails. That test applies to "significant encroachments on First Amendment rights of the sort that compelled disclosure imposes." *Human Life of Washington Inc. v. Brumsickle*, 624 F.3d 990, 1003 (9th Cir. 2010); *Mayer*, 503 F.3d at 748. However, the underlying premise of Plaintiffs' summary judgment motion—that the program exposes to government scrutiny their identities and sensitive contacts with members, supporters, and constituents—is without foundation. As explained above, the metadata collected do not reveal Plaintiffs' names or addresses or that of anyone with whom they speak, Shea Decl. ¶¶ 7, 15, 18, 21, and, regardless, Plaintiffs offer no evidence that metadata related to their communications have ever been accessed or reviewed by NSA analysts

for any purpose, whether as the results of queries based on the "reasonable, articulable suspicion" standard, or otherwise.[27] Nor do Plaintiffs plausibly allege that the challenged program is content-based, much less directed at curtailing or punishing free speech or association. Indeed, numerous safeguards built into the program prevent the Government from acquiring or using the data for purposes forbidden by the First Amendment.[28]

Nor can Plaintiffs draw any meaningful parallel between this case and compelled disclosure cases where courts have applied exacting scrutiny to government conduct. In *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), on which Plaintiffs principally rely, Pls.' Mem. at 18-19, the Alabama courts had ordered the NAACP to produce local membership lists (containing names and addresses of all members) in connection with litigation to oust it from the State as an unregistered corporation. *Id.* at 451-53. The Supreme Court held that Alabama could not compel the NAACP to disclose its lists because it "made an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.* at 462. "Under these circumstances," the Court found it "apparent that compelled disclosure of [NAACP]'s Alabama membership" entailed a "substantial restraint" on the organization's freedom of association. *Id.*; *see Brown v. Socialist Workers '74 Campaign Comm.*, 459 U.S. 87, 98-99 (1982) (similarly holding unconstitutional the targeted, compelled disclosure of contributions to and expenditures by Socialist Workers Party, based on "substantial

[27] Even if the program did reveal such information—which it does not—it still would not violate the First Amendment. In *United States v. Gering*, the Ninth Circuit reaffirmed that a targeted mail cover did not violate a defendant's rights because "he could expect no privacy as to the outside of his incoming mail, and any 'chill' on the exercise of First Amendment rights resulting from that 'lack of privacy' is not significant enough to be constitutionally impermissible when, as here, the challenged activity [a mail cover] does not concern the substance of a communication and fits within regulatory restrictions." 716 F.2d 615, 619 (9th Cir. 1983) (quoting *United States v. Choate*, 576 F.2d 165, 181 (9th Cir. 1978)). *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 may not be read absent a warrant, the First Amendment is not violated).

[28] *See* Primary Order at 8-9 (requiring NSA General Counsel's Offfice to review all findings of reasonable, articulable suspicion for numbers reasonably believed to be used by U.S. persons to ensure the findings are not based on activities protected by the First Amendment); 50 U.S.C. § 1861(a)(1) (prohibiting any investigation of a United States person "conducted solely upon the basis of activities protected by the first amendment to the Constitution").

evidence" of harassment, threats, assaults, and reprisals against its members); *Bates v. City of Little Rock*, 361 U.S. 516, 524 (1960) (similar).

In contrast, the FISC's orders authorizing the telephony metadata program do not compel Plaintiffs, providers, or anyone else to disclose the names or addresses of Plaintiffs, their members, clients, or anyone else with whom they associate (or expose them to the public hostility suffered by the parties in such cases as *NAACP*, *Bates*, and *Brown*).[29]

C. Plaintiffs Have Failed to Meet Their Burden of Establishing a "Prima Facie Infringement" of Protected First Amendment Associational Rights

Alternatively, Plaintiffs argue that they can establish a "prima facie infringement" of their First Amendment rights of association by showing (1) that compelled disclosure of their members' identities has resulted in harassment, membership withdrawal, or the discouragement of new members; or (2) other factors objectively suggesting a "chilling" of members' associational rights. Pls.' Mem. at 20 (citing, *inter alia*, *Brock v. Local Union 375*, 860 F.2d 346 350 n.1 (9th Cir. 1988)).

Plaintiffs' statement of this test, however, is incomplete.[30] While the Ninth Circuit has outlined the test in the disjunctive, it has made clear that, for both factors, "*Brock*'s prima facie

[29] Nor can a parallel be drawn between the telephony metadata program and the compelled-disclosure statute at issue in *Shelton v. Tucker*, 364 U.S. 479 (1960), which required every public educator, as a condition of employment, to file annually an affidavit listing every organization to which he or she belonged or regularly contributed within the preceding five years. *Id.* at 480. In striking down the statute under the Due Process Clause, the Supreme Court emphasized the lack of any safeguards to prevent disclosure of personally identifying information, and pointed to objective evidence supporting a chilling effect. *Id.* at 486-87 & nn.6-7 (noting that the law did "not provide that the information it requires be kept confidential," and that the record reflected public disclosure of the information as well as evidence that a certain group sought "access to some of the Act 10 affidavits with a view to eliminating from the school system persons who supported organizations unpopular with the group," such as "the American Civil Liberties Union"); *see also Dole v. Local Union 375*, 921 F.2d 969, 974 (9th Cir. 1990) (rejecting First Amendment claim based on alleged chilling effect of disclosure where, *inter alia*, "Department [of Labor] policy protects the subpoenaed information from public disclosure").

[30] Even under Plaintiffs' recitation of the test, their summary judgment motion fails because, as explained above, the program does not compel disclosure of Plaintiffs' names or addresses or those with whom they speak. Moreover, Plaintiffs' characterization of the second prong of the test does not accurately represent Ninth Circuit law. In explaining the required showing of consequences that "objectively" suggest a chilling effect, Plaintiffs cite *California Pro-Life Council, Inc. v. Getman*, 328 F.3d 1088 (9th Cir. 2003) (*CPLC*), for the proposition that such a showing can be met "by demonstrating that the plaintiff is self-censoring by not engaging in particular communications." Pls.' Mem. at 20. The language referenced from *CPLC*, however, concerns the threshold Article III standing requirement to support a vagueness claim, not a substantive showing under the First Amendment on a motion for summary judgment. *See*

test has two tiers." *Dole v. Local Union 375*, 921 F.2d 969, 972 (9th Cir. 1990). First, Plaintiffs must establish "a causal link between the disclosure and the prospective harm to associational rights. Second, [they] must demonstrate that it is the type of association where disclosure could incite threats, harassment, acts of retribution, or other adverse consequences that could reasonably dissuade persons from affiliating with it." *Id.* Neither of these showings is made in the numerous declarations that accompany Plaintiffs' motion.

None of the declarations contains the "careful documentation of membership decline" that the "first tier" requires. *Id.* at 973.[31] Instead, they uniformly allege a tenuous temporal connection between media reports of the telephony metadata program and a decrease in constituent communication. *E.g.*, Patient Privacy Decl. ¶ 6 ("[P]rior to the revelations of NSA tracking, we received on average 40 calls per month. After the NSA revelations became public, we received on average only 20 calls per month."); *accord, e.g.*, Bill of Rights Comm. Decl. ¶ 4; Acorn Decl. ¶ 7.[32] This documentation is insufficient under Ninth Circuit law. The allegation of

---

CPLC, 328 F.3d at 1093. Indeed, it would defy logic to treat an allegation of self-censorship as an "objective and articulable fact[], which go[es] beyond broad allegations or subjective fears." *Dole*, 921 F.2d at 972 (outlining prima facie First Amendment showing).

[31] Indeed, the declarations simply paraphrase, often in rote fashion, the language describing this test as recited in Plaintiffs' legal memoranda, followed by vague and subjective allegations of harm. *Compare* Pls.' Mem. at 20, *with, e.g.*, CAL-FFL Decl. ¶ 3; Calguns Decl. ¶ 3; Free Software Decl. ¶ 3; CAIR-F Decl. ¶ 3. While some of these declarations vaguely reference a "decrease in communications from members and constituents," CAL-FFL Decl. ¶ 31, they do not allege, in any specific fashion, a reduction in membership. Furthermore, the only two declarations that attempt do so—those of First Unitarian and Media Alliance—do not objectively connect the decline to the challenged program and, at any rate, contain the very allegations deemed insufficient by the Ninth Circuit in *Dole*. *Compare* Media Alliance Decl. ¶ 9 ("Several organization members have asked to have their membership terminated . . . in the wake of *recent publicity about* the extent of telephone metadata surveillance.") (emphasis added), *and* First Unitarian Decl. ¶ 4(c) (alleging that the "threat of exposure" from prior experience with government surveillance "has caused potential visitors to stay away, and members to withdraw from the community"), *with Dole*, 921 F.3d at 973 (rejecting allegations of chill with no "objective and articulable facts" causally connecting it to challenged governmental activity).

[32] Some fail even to allege these vague temporal connections. *See* Free Press Decl. ¶ 5; First Unitarian Decl. ¶ 5; People for Am. Way Decl. ¶ 6; Franklin Armory Decl. ¶ 4. *See also, e.g.*, Free Software Decl ¶ 5 ("As a concrete example [of a chilling effect], some of our supporters are refusing to attend [our annual conference] explicitly because of surveillance."); Charity & Security Decl. ¶ 5 ("We have experienced an increase in members expressing concern about the confidentiality of the fact of their communications, among each other and with staff."). Others cite fears that stem from the mistaken belief that their "private communications may be turned over to the government" under the challenged program. Free Software Decl. ¶ 4(c). *See* Shea Decl. ¶¶ 7, 15, 21.

a decrease in communication "coincident with the start" of the program "does not satisfy the first tier of the *Brock* test. Documenting a result does not prove its cause." *Dole*, 921 F.2d at 973.

Even assuming, however, that Plaintiffs could satisfy *Brock*'s first tier, their declarations fall well short of the proof required for the second tier because they are "devoid of objective facts indicating a well-founded fear of threats, harassment, or other adverse consequences" if non-content telephony metadata related to their calls were disclosed. *Id.* These declarations broadly and subjectively "argu[e], rather than factually document[] an alleged chill of associational freedom," *id.* at 974, and entirely fail to connect the alleged chill to the challenged program,[33] much less "establish that . . . members legitimately feared retribution by those few governmental employees who would have access to its records," *id.* Nor do they explain "how [their] subjective fear[s] . . . could be realized, given that" where any metadata are collected under the program, the statutory framework and FISC-ordered minimization requirements "protect[ ] the [metadata] from public disclosure," as explained above. *Id.* at 974; *Perry v. Schwarzenegger*, 591 F.3d 1126, 1140 n.6 (9th Cir. 2010) ("A protective order limiting the dissemination of disclosed associational information may mitigate the chilling effect and could weigh against a showing of infringement."); *McLaughlin v. Serv. Emps. Union*, 880 F.2d 170, 175 (1989). For each of these reasons, Plaintiffs have failed to adduce sufficient evidence to establish a prima facie case of First Amendment infringement.[34]

---

[33] *See, e.g.*, First Unitarian Decl. ¶ 8 (explaining why "spying makes people afraid to belong to the church community"); CAIR-F Decl. ¶ 3; UUSC Decl. ¶ 3 ("We believe that these partners are now hesitant to contact our organization or speak freely as a result of the NSA's dragnet surveillance"); Free Press Decl. ¶¶ 3-5. To the extent any declarants actually point to prior incidents of alleged government misconduct, those incidents did not involve the collection of third-party telephony metadata or any activity resembling the challenged program. *See, e.g.*, Bill of Rights Comm. Decl. ¶ 8(a) (basing present fear on prior "police violence and misconduct in the context of prior restraints on First Amendment activity"); Shalom Center Decl. ¶ 5 (basing present fear on being personally subject to "warrantless searches, theft, [and] forgery[] by the FBI between 1968 and 1974"); First Unitarian Decl. ¶ 4 (basing present fear on subpoenas issued to members by the House Un-American Activities Committee "[i]n the 1950s" or hearing "personal stories of [immigrant church members] being physically tortured at the hands of their [foreign] government").

[34] Even assuming, *arguendo*, that Plaintiffs could establish a prima facie case, the Government has clearly met its burden of showing "(1) that the information sought . . . is rationally related to a compelling governmental interest"—namely, identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks—and "(2) that the government's disclosure requirements are the 'least restrictive means' of obtaining the desired information." *Dole v. Serv. Emps. Union*, 950 F.2d 1456, 1461 (9th Cir. 1991) (internal quotations omitted).

VI. PLAINTIFFS FAIL TO STATE DUE PROCESS CLAIMS

Plaintiffs' substantive due process claim is premised on an alleged liberty interest in the privacy of their communications. *See* FAC ¶¶ 90-92. However, "[w]here a particular Amendment 'provides an explicit textual source of constitutional protection' against a particular sort of government behavior, 'that Amendment, not the more generalized notion of "substantive due process," must be the guide for analyzing' these claims." *Albright v. Oliver*, 510 U.S. 266, 273 (1994) (quoting *Graham v. Connor*, 490 U.S. 386, 395 (1989)); *Ramirez v. Butte-Silver Bow Cnty.*, 298 F.3d 1022, 1029 (9th Cir. 2002). Because Plaintiffs ground their substantive due process claim on privacy interests allegedly protected by the Fourth Amendment, that claim must be dismissed. *Accord Galbraith v. Cnty. of Santa Clara*, 307 F.3d 1119, 1127 (9th Cir. 2002).

Plaintiffs also fail to state a viable procedural due process claim. They argue that the Government deprived them of the aforementioned privacy interests by seizing, collecting, searching and using telephony metadata related to their communications without providing any pre-deprivation notice that would allow Plaintiffs to ascertain "specifically what conduct may subject them to electronic surveillance." FAC ¶¶ 91-92, 95-96; *see also id.* ¶ 97 (alleging, for same reasons, that 50 U.S.C. § 1861 is unconstitutionally vague).

To establish a violation of procedural due process, Plaintiffs must show that the Government deprived them of a "constitutionally protected liberty or property interest," and a "denial of adequate procedural protections." *Kildare v. Saenz*, 325 F.3d 1078, 1085 (9th Cir. 2003). Plaintiffs cannot survive the threshold inquiry here, as they have not shown a deprivation of a constitutionally protected liberty or property interest. *See Erickson v. United States*, 67 F.3d 858, 861 (9th Cir. 1995). Although Plaintiffs assert an "informational privacy interest" in non-content telephony metadata related to their calls, FAC ¶¶ 90, 95, they have no reasonable expectation of privacy in such data, as explained *supra*, Part IV, and they do not plausibly allege any other constitutionally protected privacy interest in these data. Without the deprivation of

---

The Government has explained that the program's objectives could not be achieved as effectively by relying on the targeted collection of telephony metadata that Plaintiffs appear to suggest, whether by subpoenas, national security letters, or pen-register and trap-and-trace devices, as this would reduce the Government's ability to identify networks of previously unknown foreign terrorist operatives in the United States as rapidly, reliably, and completely as analysis of bulk telephony metadata. *See* Skule Decl. ¶¶ 9, 19-29; Shea Decl. ¶¶ 46, 57-63.

such an interest, the Due Process Clause is not implicated. *Ingraham v. Wright*, 430 U.S. 651, 672 (1977); *Johnson v. Rancho Santiago Cmty. Coll.*, 623 .3d 1011, 1029 (9th Cir. 2010).[35]

Even assuming, however, that Plaintiffs retain a residual privacy interest in non-content telephony metadata related to their calls that is entitled to due-process protection—above and beyond the protections already afforded by the Fourth Amendment—they are not "due" the pre-deprivation notice they demand. When protected liberty interests are implicated (unlike here), the determination of what process is due often requires consideration of three factors: "(1) the private interest affected by the official action; (2) the risk of an erroneous deprivation of such interest through the procedures used and probable value of additional safeguards; and (3) the Government's interest." *Fairley v. Luman*, 281 F.3d 913, 918 & n.6 (9th Cir. 2002) (citing *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976)). Due process "is not a technical conception with a fixed content unrelated to time, place and circumstances," but rather, it "is flexible and calls for such procedural protections as the particular situation demands," *Gilbert v. Homar*, 520 U.S. 924, 930 (1997) (internal quotation marks and citation omitted)), and, as relevant here, takes into account "essential national security considerations," *Gonzalez v. Freeman*, 334 F.2d 570, 580 n.21 (D.C. Cir. 1964). *See Marshall v. Sawyer*, 365 F.2d 105, 111 (9th Cir. 1966).

Here, the Government's interest in identifying and tracking terrorist operatives for the purpose of preventing terrorist attacks far outweighs any residual "informational privacy" interest that Plaintiffs may have in non-content telephony metadata related to their calls not already protected by the Fourth Amendment, and by the same token outweighs any risk of erroneous deprivation of that interest. "[N]o governmental interest is more compelling than the security of the Nation." *Haig*, 453 U.S. at 307; *see also Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2724 (2010). The NSA's collection of telephony metadata thus promotes a governmental interest of the highest order. *See, e.g., id.*; *In re Sealed Case*, 310 F.3d 717, 746 (F.I.S.C.-R. 2002). Owing to this compelling interest, Congress specifically rejected providing

[35] Plaintiffs' vagueness claim also fails for lack of a protected liberty or property interest. *See, e.g., Williams v. Vidmar*, 367 F. Supp. 2d 1265, 1275 (N.D. Cal. 2005) ("Since no constitutionally-protected activity is being restricted, there can be no claim that the procedures used to impose the restrictions are constitutionally insufficient.").

the process Plaintiffs seek.[36] Requiring the Government to provide advance notice to every individual before acquiring non-content telephony metadata related to his or her communications would be incompatible with the secrecy required for the challenged program, see *supra* Part II, and fatal to its objectives. For example, if the Government disclosed to an individual associated with a foreign terrorist organization that metadata related to his communications were to be collected and subject to scrutiny by the Government, that individual, and his or her associates, could take steps to avoid detection and alter their plans, thus placing national security at greater risk.[37] Due process does not require the Government to put national security at risk in such fashion by providing communications services subscribers the process that Plaintiffs demand. *See Holder*, 130 S. Ct. at 2727; *Haig*, 453 U.S. at 309-10; *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 980-81 (9th Cir. 2012).[38]

CONCLUSION

For the reasons stated above, Defendants' Motion to Dismiss should be granted, and Plaintiffs' Motion for Partial Summary Judgment should be denied.

---

[36] *See* 50 U.S.C. § 1861(f)(2)(A)(i) (providing only recipients the right to challenge lawfulness of Section 215 orders before the FISC); *supra* at 18-19 & n.11 *Cf. Jerry T. O'Brien, Inc.*, 467 U.S. at 742-50 (target of investigation not entitled to notice—under due process clause or otherwise—when SEC issues subpoenas to third party providers).

[37] *See, e.g.*, *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663, 679 (1974) (dispensing with pre-deprivation notice or hearing when exigent circumstances exist and the government demonstrates a "pressing need for prompt action"); *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 985 (9th Cir. 2012) ("[A]s many courts have held, the potential for 'asset flight' almost certainly justifies OFAC's decision not to provide notice before freezing the assets."); *Global Relief Found., Inc. v. O'Neill*, 207 F. Supp. 2d 779, 803 (N.D. Ill. 2002) ("Due to the exigencies of national security and foreign policy considerations, the Executive Branch historically has not provided pre-deprivation notice in sanctions programs under [the International Emergency Economic Powers Act].").

[38] Count V of the complaint, seeks "the return" of any call-detail records collected under the program about Plaintiffs' telephone communications, pursuant to Fed. R. Crim. P. 41(g). FAC ¶¶ 111-112. Rule 41(g) provides that "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Count V must be dismissed, first, because Rule 41(g) provides the basis for a motion in a criminal case, not a civil cause of action. The rule "do[es] not apply where there is no criminal proceeding connected to the seizure." *Hall v. City of Charlotte*, 2005 WL 2219326, *1 n.2 (D. Kan. Sept. 13, 2005). Moreover, the property at issue—call-detail records—does not belong to Plaintiffs but is the property of telecommunications service providers, even if it had been unlawfully searched and seized (which it has not). *See United States v. Kaczynski*, 551 F.3d 1120, 1129 (9th Cir. 2009) (defendant not entitled to return of property he never lawfully possessed).

Dated: December 6, 2013

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director
tony.coppolino@usdoj.gov

s/ Marcia Berman
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities