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
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Telephone: (202) 514-3358
Facsimile: (202) 616-8470
james.gilligan@usdoj.gov

WENDY J. OLSON, Idaho Bar No. 7634
United States Attorney
SYRENA C. HARGROVE, Idaho Bar No. 6213
Assistant United States Attorney
District of Idaho
Washington Group Plaza IV
800 E. Park Boulevard, Suite 600
Boise, ID 83712-9903
Telephone: (208) 334-1211
Facsimile: (208) 334-1414
Syrena.Hargrove@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

ANNA J. SMITH, Plaintiff, v. BARACK OBAMA, President of the United States, *et al.*, Defendants.	No. 2:13-cv-00257-BLW **MEMORANDUM IN OPPOSITION TO PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION AND IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS**

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

LEGISLATIVE MATERIAL

FEDERAL RULES 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. Plaintiff in this case asks this Court to invalidate and issue a preliminary injunction against 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, Plaintiff challenges 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 telecommunications service providers that include such information as the time and duration of calls made, and the numbers dialed, but not the content of calls or any persons' names or addresses. Collection and targeted querying of these records—which have been repeatedly authorized by the FISC as consistent with governing laws and the Constitution—permit 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.

Plaintiff nevertheless asserts that this activity is unauthorized by FISA, and violates her First and Fourth Amendment rights. For the reasons discussed herein, the Court lacks jurisdiction to entertain these claims. They also fail, in any event, to state grounds on which relief can be granted, and Plaintiff makes no showing of irreparable harm. Thus, Plaintiff's motion for a preliminary injunction should be denied, and the amended complaint dismissed.

First, Plaintiff has not established her standing to sue. Plaintiff offers no proof—only conjecture—that metadata about her communications have been collected by the NSA, much less

reviewed by NSA analysts. Indeed, 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 indiscriminate querying of the metadata, using identifiers not connected with terrorist activity, to create "detailed pictures" of the persons with whom ordinary Americans associate, as Plaintiff surmises. There is no non-speculative basis, then, to expect that query results under this standard will include information about calls either made by Plaintiff, or made to her by others.

Second, Plaintiff has satisfied none of the requirements that must be met to justify relief so extraordinary as a preliminary injunction against a long-running intelligence program conducted for the protection of national security. Plaintiff's Fourth Amendment claim, the sole legal ground on which she bases her request for preliminary relief, fails because telephone subscribers have no protected privacy interest in the kind of non-content information at issue here, as the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), as recently held by the FISC, and as held by two district courts in rejecting constitutional challenges to the telephony metadata program. Moreover, even if Plaintiff had a protected privacy interest in telephony metadata, she has not shown an infringement of that interest through actual review by NSA analysts of metadata pertaining to her calls. And even if the Government's conduct implicated a protected Fourth Amendment interest, the NSA's FISC-authorized collection and review of bulk telephony metadata is "reasonable" and permissible in light of the strong national interest in preventing terrorist attacks, and the minimal intrusion on individual privacy. Furthermore, apart from Plaintiff's failed claim that her Fourth Amendment rights are being violated, she makes no showing that she has suffered any tangible consequences attributable to the program, much less injury that would qualify as irreparable harm. For much the same reasons, the balance of harms

and the public interest weigh heavily against issuing an injunction that would interfere with the operation of a long-running and important national security program.

Third, Plaintiff's claims must be dismissed, because none of them (including her Fourth Amendment claim) plausibly states an entitlement to relief. Review of Plaintiff's claim that the telephony metadata program exceeds the Government's authority under FISA is precluded, *inter alia*, by FISA's detailed scheme for judicial review of specified intelligence activities, as both courts to consider the issue have held. Further, as the FISC has repeatedly found—and so, too, the sole district court to reach the question—the NSA's bulk collection of telephony metadata is authorized under FISA, because there are reasonable grounds for believing that the metadata as a whole are relevant to authorized FBI counter-terrorism investigations. Plaintiff also fails to state a First Amendment claim, because she has neither alleged nor shown that the telephony metadata program infringes on her expressive or associational activities, and because good-faith investigative activity, such as this program, conducted without purpose to deter or punish protected speech or association, does not violate the First Amendment.

On January 17, 2014, the President announced a number of reforms to the Nation's intelligence programs, including the telephony metadata program, many of which are designed to enhance already existing protections for individual privacy. In so doing, the President stated his belief that "it is important that the capability that this program is designed to meet is preserved." Plaintiff has made no showing that would justify a contrary result in this case.

STATEMENT OF FACTS

Statutory Background

Congress enacted FISA to authorize and regulate certain Government surveillance of communications and other activities for purposes of gathering foreign intelligence. 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 authorizes the FISC, an Article III court composed of 11 appointed U.S. district judges, *see* 50 U.S.C. § 1803, 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 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), and 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 the investigation in question. *Id.* § 1861(b)(2)(A).

Information contained in the records or other 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 need . . . to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1861(b)(2)(B), (g)(2), (h). The FISC must find these requirements have been met before it issues the requested order, which must direct that the minimization procedures set forth in the application be followed. *Id.* § 1861(c)(1).

Section 215 includes a scheme providing for judicial review of production orders, 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). FISA does not provide for review of Section 215 orders at the behest of third parties.

The Collection and Review of Bulk Telephony Metadata Authorized by the FISC

Plaintiff challenges 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) has since May 2006 obtained orders from the FISC under Section 215 directing certain telecommunications service providers to produce to the NSA, on a daily basis, electronic copies of "call detail records containing 'telephony metadata,'" created by the recipient providers for calls to, from, or wholly within the United States. The NSA has then stored and queried 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-five 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

[1] Declaration of Teresa H. Shea (Shea Decl.) ¶¶ 13-14, 16-17, 20 (Exh. A); Declaration of John Giacalone ("Giacalone Decl.") ¶¶ 3, 6 (Exh. B); *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, Dkt. No. BR 13-109 (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. BR 13-80, 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. BR 13-80 (F.I.S.C. Apr. 25, 2013) ("Secondary Order") (Exh. F) at 1-2, 4.

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; *see also* Giacalone Decl. ¶¶ 7, 11.

The Government has obtained 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. *Id.* ¶ 10; *see* 50 U.S.C. § 1861(a)(1), (b)(2)(A). As required by Section 215, each 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. Giacalone Decl. ¶ 10. FISC orders authorizing the collection are based on the court's findings that there are "reasonable grounds to believe 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; Giacalone Decl. ¶ 8; Shea Decl. ¶¶ 29-36. Under the restrictions ordered by the FISC since the program's inception, NSA analysts have been permitted to review the metadata for purposes of obtaining foreign intelligence information, and may do so only through electronic "contact-chaining" queries 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 could 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 was reasonably believed to be used by a U.S. person, NSA's Office of General Counsel had to determine that the term was not regarded as associated with a foreign terrorist group solely on the basis of activities protected by the First Amendment. Shea Decl. ¶¶ 20-24, 32; Primary Order at 6-9. The requirement of "reasonable, articulable suspicion" 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 have never been 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. ¶¶ 24-27.

Since the program's inception, results of approved queries have been 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 could only include identifiers and associated metadata having direct contact with the seed (the first "hop"), identifiers and associated metadata having direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having direct contact with second "hop" identifiers (the third "hop"). *Id.* ¶¶ 23, 28. Query results do not include the names or addresses of persons associated with the responsive telephone numbers, because that information is not included in the database in the first place. *Id.* ¶ 22.

The NSA's ability under this program to accumulate metadata in bulk, and to quickly conduct contact-chaining 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 at multiple hops from the seed identifier 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, which can be immediately performed as new terrorist-associated identifiers come to light. *Id.* ¶¶ 47-51, 58-65; Giacalone Decl. ¶¶ 27-29.[2]

In addition to the above 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.

On January 17, the President announced a series of reforms to the Nation's intelligence programs. Regarding the telephony metadata program, the President ordered a transition during which the Government is to develop options for a new approach that can preserve the program's

[2] Under the FISC's orders, the NSA may share query results to allow Government investigators to discover persons who have been in contact with known or suspected terrorist groups, and may themselves be engaged in terrorist activity. The NSA, however, does not indiscriminately provide the FBI with all identifiers connected at one or more hops from a suspected terrorist identifier. Rather, NSA applies signals intelligence tradecraft to focus only on those identifiers which may be of use to the FBI in detecting persons in the United States who may be associated with the specified foreign terrorist groups. Shea Decl. ¶¶ 24, 27, 29.

capabilities without the Government holding the bulk telephony metadata itself. The President also directed that, effective immediately, (1) the NSA will review metadata only within one or two "hops" of a seed identifier, not three; and (2) the Government will work with the FISC so that, during the transition period, seed identifiers based on "reasonable, articulable suspicion" can be used only after a judicial finding or in a case of true emergency. Remarks by the President on Review of Signals Intelligence ("President's Remarks") (Exh. G). The Government is taking immediate action to implement these reforms. Shea Decl. ¶¶ 23, 32, 38.

Plaintiff's Allegations

Plaintiff filed this action on June 12, 2013 (ECF No. 1), but never served her initial complaint. Plaintiff filed her amended complaint on November 7, 2013 (ECF No. 3), and on December 20, 2013, more than six months after bringing suit, moved for a preliminary injunction. Pl.'s Mot. for a Prelim. Inj. (ECF No. 8) ("Pl's PI Mot.").

According to Plaintiff's Amended Complaint ("Am. Compl."), and the Declaration of Anna J. Smith (ECF No. 8-2) ("A. Smith Decl."), Plaintiff Anna J. Smith has been a customer of Verizon Wireless for at least the past three years. Am Compl. ¶¶ 7-8; A. Smith Decl. ¶ 2. On this basis she asserts that telephony metadata of her calls have been collected "pursuant to the April 25, 2013 Secondary Order, its predecessors and, now, its successors." Mem. in Support of Pl.'s Mot. for a Prelim. Inj. (ECF No. 8-1) ("Pl.'s PI Br.") at 7. She acknowledges, however, that the now-expired Secondary Order was issued to Verizon Business Network Services, Inc. (which, as discussed below, is a separate corporate entity from Verizon Wireless) and alleges on information and belief that "a similar order was issued to Verizon Wireless." Am. Compl. ¶¶ 15-16. Plaintiff offers no proof of this allegation and concedes, in fact, that "whether Verizon Wireless is compelled to provide metadata information to the NSA" under the program "remain[s] classified." Pl.'s PI Br. at 5 n.2. She also alleges that "[e]ven if Verizon Wireless

was not ordered to produce the metadata by the FISC, the government still captures [her] personal information because 'nearly all calls eventually travel over networks owned by U.S. companies that work with the NSA,'" Am. Compl. ¶ 17 (quoting Wall St. J., June 14, 2013)—but again offers no evidence substantiating this allegation. She also maintains in her brief that for the telephony metadata program to be effective, the NSA must be collecting metadata on "all domestic cell phones," including hers, citing a Government white paper which (as discussed below) says nothing of the kind. Pl.'s PI Br. at 9-10.

Plaintiff also asserts that metadata of her calls have been "searched" and "monitored" on the theory that the Government "must search" the metadata of all calls in the database every time it conducts a query for contacts with suspected terrorist identifiers. *Id*. at 10-11. In support of this assertion she again relies on the Government's white paper, which explains, to the contrary, that "the vast majority of [the metadata are] never seen by any person," because "[o]nly [metadata] responsive to the limited queries that are authorized for counterterrorism purposes [are] extracted and reviewed by analysts." *See id*.

Plaintiff contends that she has a subjective and reasonable expectation that metadata showing whom she calls and when will not be "gathered, stored and monitored by" the Government, Am. Compl. ¶¶ 21-23; A. Smith Decl. ¶¶ 6-9, and "felt [it] was a violation of [her] privacy rights" when she "learned" that this information was allegedly "being shared with the government." A. Smith Decl. ¶¶ 9-10. Plaintiff otherwise alleges no Government review or dissemination of information about herself or persons with whom she communicates, or that she has suffered consequences of any kind as a result of Defendants' alleged actions.

Plaintiff contends that the telephony metadata program exceeds the Government's authority under Section 215, and violates the First and Fourth Amendments to the Constitution. Am. Compl. ¶¶ 25-27. She seeks declaratory and injunctive relief, *id*., Prayer for Relief ¶¶ 2-5,

including a preliminary injunction that, during the pendency of this suit, (i) bars Defendants from collecting records of her calls under the telephony metadata program, (ii) requires Defendants to "quarantine" all such records already collected, and (iii) prohibits queries using any phone number or other identifier associated with her. Pl.'s PI Mot. at 2.

ARGUMENT

I. PLAINTIFF HAS NOT CARRIED HER BURDEN OF ESTABLISHING HER STANDING TO CHALLENGE THE TELEPHONY METADATA PROGRAM

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), and a demonstration of a plaintiff's standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). The standing inquiry must be "especially rigorous" when reaching the merits of a claim would force a court to decide the constitutionality of actions taken by a coordinate Branch of the Federal Government in the field of intelligence gathering. *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1147 (2013).

To establish her standing, Plaintiff must show that she has suffered an injury in fact, fairly traceable to the challenged actions of the Defendants and redressable by a favorable ruling, that is "concrete, particularized, and actual or imminent." *Id.* Any "threatened injury must be *certainly* impending to constitute injury in fact," whereas "allegations of *possible* future injury are not sufficient." *Id.* (internal quotations and alterations omitted). Plaintiff must show that she has standing "with the manner and degree of evidence required at the successive stages of the litigation," *Defenders of Wildlife*, 504 U.S. at 561, meaning that, in opposition to Defendants' motion to dismiss, she cannot rely on "conclusory and barebones" allegations in her complaint,

Perez v. Nidek Co., 711 F.3d 1109, 1113 (9th Cir. 2013), and in support of her request for injunctive relief must submit competent evidence to prove her standing. *See K-2 Ski Co. v. Head Ski Co.*, 467 F.2d 1087, 1088 (9th Cir. 1972); Charles Alan Wright, Arthur Miller et al., Fed. Prac. & Proc. § 2949 (2013). If she cannot carry these threshold jurisdictional burdens, then "the [C]ourt cannot proceed" and must grant Defendants' motion to dismiss, and deny her motion for a preliminary injunction. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94, 101 (1998).

B. Plaintiff Has Not Established Her Standing

Plaintiff has failed to allege or demonstrate an injury meeting Article III's standards. Plaintiff asserts that, because she is a Verizon Wireless customer, metadata associated with her calls must be "gathered" by and "shared with the government," Am. Compl. ¶ 22; A. Smith Decl. ¶¶ 2, 9, and that records pertaining to her calls are searched every time the NSA runs a query of its database. *See* Pl.'s PI Br. at 10-11. Neither contention is sufficient to establish her standing.

1. Plaintiff Has Not Shown That Metadata Associated With Her Calls Have Been Collected

As an initial matter, Plaintiff merely speculates, but has not shown, that metadata associated with her phone calls have been collected by the NSA. Initially she contends that metadata of her calls must have been collected based on "information and belief" that her telephone service provider, Verizon Wireless, participates in the telephony metadata program. *Id.* at 7. Yet she offers no proof of this assertion, and, except for a single, now-expired Secondary Order issued on April 25, 2013, to Verizon Business Network Services, Inc.—a separate business entity from Verizon Wireless, *see, e.g., United States ex rel. Shea v. Verizon Bus. Network Servs., Inc.*, 904 F. Supp. 2d 28, 30 (D.D.C. 2012)—the Government has not declassified or otherwise acknowledged any further information regarding the identities of any other participating providers, past or present. *See* Shea Decl. ¶ 17. That includes whether

Plaintiff's provider, Verizon Wireless, is now or ever has been a participating provider in the program, as Plaintiff acknowledges. Pl's PI Br. at 5 n.2 ("aspects of the program remain classified, including whether Verizon Wireless is compelled to provide metadata information to the NSA"); *see also* Administration White Paper ("White Paper") (P. Smith Decl., Exh. 4) at 1; Shea Decl. ¶ 5; Giacalone Decl. ¶ 3. The consequences of that omission from the record befall Plaintiff, as it is her "burden to prove [her] standing by pointing to specific facts, not the Government's burden to disprove standing by revealing details" of its intelligence programs. *Amnesty Int'l, USA*, 133 S. Ct. at 1149 n.4.

Plaintiff also alleges that, even if Verizon Wireless were not a participant in the program, the collection from the "companies that work with the NSA" (which she does not identify) still encompasses records of "nearly all calls." Am. Compl. ¶ 17. Again, Plaintiff offers no proof or even supporting allegations for this conclusion. Instead, she argues that "the government has essentially conceded" that it is collecting metadata associated with "all domestic cell phones," including hers, because it has acknowledged that otherwise the program would not be effective. Pl.'s PI Br. at 9-10. That is not so, on either score. While the Government has acknowledged that the program is broad in scope and involves the aggregation of an historical repository of data collected from more than one provider, the Government has not stated, nor is it correct, that the program captures information about all—or even virtually all—telephone calls to, from, or within the United States. *See* Shea Decl. ¶ 17; *see also* Aug. 29 FISC Op. at 4 n.5 ("[P]roduction of all call detail records of all persons in the United States has never occurred under this program."). Yet the program's utility and effectiveness are a matter of record. *See* Shea Decl. ¶¶ 47-65; Giacalone Decl. ¶¶ 17-26; *ACLU v. Clapper*, 2013 WL 6819708, at *25-26 (S.D.N.Y. Dec. 27, 2013). Similarly, the White Paper does not, as Plaintiff suggests, state that "collecting metadata from all domestic cell phones [is] imperative to the potency of the program." Pl.'s PI

Br. at 9. Rather, the Government has simply explained that collection only of known terrorists' communications would not give the NSA the same capability to detect and identify *unknown* terrorist operatives. *See* White Paper at 12-13; Shea Decl. ¶¶ 60-64.

At bottom, Plaintiff's speculation about which providers "must" be participating in the program, and how much metadata "must" be collected to achieve some unspecified standard of "effectiveness," is simply not sufficient to establish that metadata pertaining to Plaintiff's calls have been collected by the NSA. Plaintiff has thus failed to establish her standing with the rigor required in extraordinary litigation implicating national security. *See Amnesty Int'l, USA*, 133 S. Ct. at 1147-48 (speculation that an injury in fact has occurred or may occur is insufficient to confer standing to challenge lawfulness of a Government intelligence program).

2. Plaintiff Has Not Shown That Metadata Associated With Her Calls Have Been Reviewed, "Searched," or "Monitored"

Presuming that records of her calls have been collected, Plaintiff also asserts that she has standing to challenge alleged NSA "monitoring" and "searches" of the metadata associated with calls she makes and receives. *See* Am. Compl. ¶¶ 21-22; Pl.'s PI Br. at 10-11. 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 7; Primary Order at 7; Shea Decl. ¶ 21. As a result, only a "tiny fraction" of the records are ever seen by any person. Shea Decl. ¶ 24; White Paper at 4, 15. Plaintiff's amended complaint contains no well-pleaded, non-conclusory allegations, much less has Plaintiff adduced evidence, that allegedly collected records of her calls are among the very small percentage that NSA has 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

Plaintiff either have been or ever will be reviewed by the NSA. *See Amnesty Int'l, USA*, 133 S. Ct. at 1148 (holding that a plaintiff cannot establish standing to challenge a Government surveillance program when it is "speculative whether the Government will imminently target communications to which [the plaintiff is a] part[y]").

Seeking to avoid this conclusion, Plaintiff argues that metadata associated with her calls is "searched" every time "the government queries the database,"Pl.'s PI Br. at 10-11, but that is not the case. The NSA conducts queries of its database electronically, not by manual review of the metadata contained in each record. When the NSA runs queries of the database, they result in no records; the analysts see no metadata associated with anyone's calls; and, thus, they learn nothing about the communications of particular individuals, unless their telephone numbers (or other identifiers) fall within the authorized number of "hops" from a targeted terrorist identifier. *See* Shea Decl. ¶¶ 22, 24, 28. Plaintiff cites no support for the proposition that electronic queries resulting in no information about her communications can be taken as "searches" or "monitoring" of information pertaining to her calls, and the theory is cast into doubt by substantial authority.[4] Thus, absent evidence that NSA queries of the database have resulted in information about Plaintiff's communications, she can point to no review of metadata allegedly collected about her calls that would support her standing. For this reason as well, Plaintiff's claims must be dismissed, and her motion denied.

[4] *See United States v. Jacobsen*, 466 U.S. 109, 123 (1984) ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy"); *United States v. Place*, 462 U.S. 686, 707 (1983) (canine sniff of luggage that reveals "only the presence or absence" of narcotics without otherwise revealing the contents is not a search under the Fourth Amendment). *See also Horton v. California*, 496 U.S. 128, 142 n.11 (1990) (governments acquisition of an item without examining its contents "does not compromise the interest in preserving the privacy of its contents"); *United States v. Van Leeuwen*, 397 U.S. 249, 252-53 (1970) (defendant's interest in the privacy of his detained first-class mail "was not disturbed or invaded" until the Government opened the packages).

II. PLAINTIFF'S PRELIMINARY INJUNCTION MOTION SHOULD BE DENIED

Even if Plaintiff had established her standing, her motion for a preliminary injunction should still be denied. To obtain a preliminary injunction, Plaintiff must "make a clear showing," *Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997), that she is entitled to such "an extraordinary and drastic remedy," which is "never awarded as of right." *Munaf v. Geren*, 553 U.S. 674, 689-90 (2008) (quotation marks and citations omitted). Plaintiff "must establish that [she] is likely to succeed on the merits, that [she] is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [her] favor, and that an injunction is in the public interest." *Winter v. NRDC*, 555 U.S. 7, 20 (2008). "The requirements are stated in the conjunctive so that all four elements must be established to justify injunctive relief." *Battelle Energy All., LLC v. Southfork Sec., Inc.*, --- F. Supp. 2d ---, 2013 WL 5828559, at *2 (D. Idaho Oct. 29, 2013) (Winmill, J.). Alternatively, under the "sliding scale" approach (which the Ninth Circuit has held survives *Winter*), a preliminary injunction may be granted when there are "serious questions going to the merits and a hardship balance that tips sharply toward the plaintiff," so long as "the other two elements of the *Winter* test are also met." *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131-35 (9th Cir. 2011).

Under either approach, a "more stringent standard is applied" where, as here, a plaintiff seeks mandatory relief upsetting, rather than maintaining, the status quo. *See Marlyn Nutraceuticals, Inc. v. Mucos Pharma*, 571 F.3d 873, 879 (9th Cir. 2009). Courts are "extremely cautious," *Battelle Energy All., Inc.*, 2013 WL 5818559, at *2, about granting this "particularly disfavored" form of relief, *Anderson v. United States*, 612 F.2d 1112, 1114 (9th Cir. 1979), and will deny a request for a mandatory injunction "unless extreme or very serious damage will result" if no injunction is issued. *Marlyn Nutraceuticals, Inc.*, 571 F.3d at 879 (internal

quotation omitted). Plaintiff has not made the showing required under these standards to obtain the truly extraordinary preliminary relief she seeks.

A. Plaintiff Is Unlikely to Succeed on the Merits of Her Claim That the Telephony Metadata Program Violates Her Fourth Amendment Rights

First, Plaintiff's Fourth Amendment claim, the sole count of the complaint on which she bases her motion, fails to state a claim upon which relief can be granted, much less does it exhibit a likelihood of success on the merits. The legal foundation of her Fourth Amendment claim—that she has a reasonable expectation of privacy in telephony metadata—is foreclosed by the controlling and squarely applicable authority of *Smith v. Maryland*, 442 U.S. 735 (1979), as two other district courts and the FISC have recently held. *ACLU*, 2013 WL 6819708, at *20-22; *United States v. Moalin*, 2013 WL 6079518, at *6-8 (S.D. Cal. Nov. 18, 2013); *see also* Aug. 29 FISC Op. at 6-9. Even if Plaintiff had a protected privacy interest in the metadata contained in business records belonging to her provider, she has not shown as a factual matter that any such interest of hers has been infringed by actual review of any metadata pertaining to her calls.

1. Plaintiff Has No Protected Privacy Interest in Telephony Metadata

The Fourth Amendment provides 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."[5] It was understood "for most of our history … 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). Since the decision in *Katz v. United*

[5] The Government's collection of bulk telephony metadata pursuant to orders of the FISC does not constitute a "seizure" of individual subscribers' records, because the orders are directed to telecommunications service providers, not to subscribers, and direct the production of what are indisputably the providers' own business records. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976) (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); *ACLU*, 2013 WL 6819708, at *21.

States, 389 U.S. 347 (1967), however, it has been understood that a Fourth Amendment "search" also takes place when the government's investigative activities "violate a person's 'reasonable expectation of privacy.'" *Jones*, 132 S. Ct. at 949-50 (quoting *Katz*, 389 U.S. at 360).

The Supreme Court squarely held, however, in *Smith v. Maryland*, 442 U.S. 735, 741-46 (1979), that "individuals have no 'legitimate expectation of privacy' regarding the telephone numbers they dial because they knowingly give that information to telephone companies when they dial a number." *ACLU*, 2013 WL 6819708, at *20. In *Smith*, the police requested (without a warrant or court order) that the telephone company install a pen register device at its central offices to record the numbers dialed from a robbery suspect's (Smith's) home phone. *Smith*, 442 U.S. at 737. After Smith was arrested, he sought to suppress evidence derived from the pen register as a violation of his Fourth Amendment rights. The Court held that even if Smith harbored a subjective expectation that the phone numbers he dialed would remain private, that expectation was not reasonable, explaining that the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44 (citing, *inter alia*, *Miller*, 425 U.S. at 441-43 (no reasonable expectation of privacy in financial records a depositor voluntarily provided to his bank)). 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." *Id*. at 743. By using his phone, Smith "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore "assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744;

see also id. at 745; *Miller*, 425 U.S. at 443 ("depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").[6]

So too, for Plaintiff. She does not allege, nor could she plausibly allege, that she did not voluntarily convey and expose phone numbers to her telephone company each and every time she used her cell phone. What she claims is that she did not expect that those numbers would be shared with the Government. A. Smith Decl. ¶¶ 6-8. But *Smith* holds that this expectation is not reasonable in light of the fact that Plaintiff voluntarily conveyed the phone numbers she dialed to her phone company—by doing so, Plaintiff "assumed the risk that the company would reveal to [the Government] the numbers [s]he dialed." *Smith*, 442 U.S. at 744. This is true even if there was an understanding that Plaintiff's phone company would treat the phone numbers she dialed as confidential. *See* A. Smith Decl. ¶ 10; *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *Miller*, 425 U.S. at 443. *Smith* therefore forecloses Plaintiff's claim that the alleged disclosure to the NSA of metadata about her calls violates her Fourth Amendment rights. *See also ACLU*, 2013 WL 6819708, at *20; *Moalin*, 2013 WL 6079518, at *6-8 (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 (*Smith* and its progeny "have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years"); *cf. [Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order (F.I.S.C. [redacted]) (declassified

[6] The third-party doctrine has consistently been applied to call detail records like the records at issue here. *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).

and released on Nov. 18, 2013) (Exh. G) ("*[Redacted]*") at 58-66 (bulk collection of Internet metadata does not violate the Fourth Amendment).

Like the court in *Klayman v. Obama*, 2013 WL 6571596 (D.D.C. Dec. 16, 2013), Plaintiff attempts to distinguish *Smith* by pointing to various factual differences between *Smith* and the instant case. But those factual differences are immaterial to *Smith's* reasoning—that an individual has no reasonable expectation of privacy in information provided to third parties. First, Plaintiff contends that Smith was suspected of a crime, whereas the telephony metadata here is collected without individualized suspicion of crime. Pl.'s PI Br. at 13. This difference has nothing to do with whether individuals, be they criminal suspects or not, have a reasonable expectation of privacy in telephony metadata for purposes of the threshold Fourth Amendment determination of whether a "search" has occurred. *See Smith*, 442 U.S. at 742; *ACLU*, 2013 WL 6819708, at *20. Instead, the question of whether individualized suspicion is required by the Fourth Amendment is part of the reasonableness analysis that is conducted *after* a court finds a search to have occurred. *See, e.g.*, *Klayman*, 2013 WL 6571596, at *23.

Second, Plaintiff argues that the circumstances here are distinguishable from *Smith* because *Smith* involved only the collection of the phone numbers dialed, not also the phone numbers from which calls are received, when the calls took place, and how long the calls lasted. Pl.'s PI Br. at 13. This argument is meritless. Just as Plaintiff voluntarily turns over the phone numbers she dials to her phone company, she voluntarily turns over the dates, times, and durations of her calls. The remaining data collected under the telephony metadata program, such as the numbers from which she receives calls, and trunk identifiers, is information collected or generated by the phone companies themselves. *See* Primary Order at 3 n.1. Thus, the rationale of *Smith* fully applies to all of the telephony metadata at issue here. *See United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009) (because data about call origination, length, and time of call

"is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy,'" citing *Smith*); *Forrester*, 512 F.3d at 510 (holding that computer surveillance techniques revealing the to/from addresses of email messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account, "are constitutionally indistinguishable from the use of a pen register . . . approved in *Smith*.").

Third, Plaintiff claims that *Smith* is distinguishable because it involved collection of the phone numbers dialed by only one person, as opposed to "hundreds of millions of people." Pl.'s PI Br. at 14. But, as the *ACLU* court recently noted, even "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search." 2013 WL 6819708, at *22. 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 Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978). No Fourth Amendment interest of Plaintiff is implicated, therefore, by the fact that the metadata of many other individuals' calls are collected as well as (allegedly) her own. *See United States v. Dionisio*, 410 U.S. 1, 13 (1973) (where single grand jury subpoena did not constitute an unreasonable seizure, it was not "rendered unreasonable by the fact that many others were subjected to the same compulsion"); *In re Grand Jury Proceedings*, 827 F.2d 301, 305 (8th Cir. 1987) ("[T]he fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation."); *United States v. Rigmaiden*, 2013 WL 1932800, at *13 (D. Ariz. May 8, 2013) (Government did not violate defendant's Fourth Amendment rights by collecting a high volume (1.8 million) of IP addresses); Aug. 29 FISC Op. at 8-9.

Indeed, the investigative activity in *Smith* was more invasive of individual privacy, not less, than in Plaintiff's case, because in *Smith* the police targeted the phone calls of a single,

known individual (Smith), examined the data gathered to ascertain whether he had contacted another known individual (his victim), and used that information to arrest and prosecute him. 442 U.S. at 737. The Court nonetheless ruled that he had no reasonable expectation of privacy in telephone numbers he dialed. *Id*. at 741-42. Here, by contrast, Plaintiff can point to no equivalent intrusion on her privacy. She has not shown that any metadata of her phone calls have ever been examined by NSA analysts. The NSA can only query the database of call detail records with a "seed" phone number, or identifier, if there is reasonable articulable suspicion that the identifier is associated with a foreign terrorist organization approved for targeting by the FISC. Shea Decl. ¶¶ 18, 20-21. When the NSA makes a query, it can review metadata only within two (previously three) "hops" of the seed. *Id.* ¶¶ 23-24. Even if any allegedly collected records of Plaintiff's calls have been among the tiny fraction of the records ever reviewed by NSA analysts, *see supra* at 7, the call detail records collected by the NSA reveal only phone numbers and other routing information, not the names, addresses, or other identifying information of parties to the calls. *See* Shea Decl. ¶¶ 15, 22; Giacalone Decl. ¶¶ 7, 11; *ACLU*, 2013 WL 6819708, at *21. As the court in *ACLU* correctly found, "without resort to additional techniques, the Government does not know who any of the telephone numbers [collected under the telephony metadata program] belong to." *ACLU*, 2013 WL 6819708, at *21. Plaintiff can complain of no putative invasion of privacy of the kind experienced by the petitioner in *Smith.*

Fourth, Plaintiff seeks to distinguish *Smith* based on the emergence of the "digital age," relying on concurring opinions in *Jones* that grappled with the impact of technological advances on the Court's Fourth Amendment jurisprudence. Pl.'s PI Br. at 13-14; *see also ACLU*, 2013 WL 6819708, at *22. Plaintiff's reliance on the *Jones* concurrences is misplaced, for multiple reasons. First and foremost, *Jones* did not overrule *Smith*, and this Court is bound by it. As the *ACLU* court explained, "the Supreme Court has instructed lower courts not to predict whether it

would overrule a precedent even if its reasoning has been supplanted by later cases" (which has not occurred here). *Id.* at *22 (citing *Agostini v. Felton*, 521 U.S. 203, 237 (1997)).

Moreover, the concerns expressed in the *Jones* concurrences about GPS monitoring do not apply here. *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring) (GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual association."); *id.* at 964 (Alito, J., concurring in the judgment) (opining that use of GPS technology to "secretly monitor and catalogue every single movement of an individual's car for a very long period" impinges on expectations of privacy). These concerns do not apply to the telephony metadata program, because of the individualized nature of the GPS monitoring at issue in *Jones*. Like the pen register in *Smith*, the GPS device used in *Jones* was attached by law enforcement officers to a single, known person's vehicle and recorded the vehicle's locations over a period of time. Law enforcement personnel examined the GPS data to ascertain where that particular person had been over 28 days and used that information to prosecute him. Here, as discussed above, there is no evidence that any metadata of Plaintiff's calls have even been reviewed, much less scrutinized in the fashion of the GPS data used by law enforcement officials to ascertain Jones' whereabouts.

Fifth, Plaintiff relies on the growth of cell phone usage to distinguish *Smith*, arguing that "[t]he huge growth in cell phone use means that the government collects, retains and queries metadata that 'reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations.'" Pl.'s PI Br. at 15 (quoting *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).[7] The court in *ACLU* aptly disposed of this argument:

[7] It was recognized in *Smith* itself that, even in 1979, a list of telephone numbers dialed "could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life," *Smith*, 442 U.S. at 748 (Stewart, J., dissenting), yet the Court ruled that there is no reasonable expectation of privacy in telephone numbers dialed.

"Telephones have far more versatility now than when *Smith* was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata," *ACLU*, 2013 WL 6819708, at *22, the only type of data at issue here. As recognized in *Klayman* (on which Plaintiff heavily relies), "what metadata *is* has not changed over time. As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like." 2013 WL 6571596, at *21.[8]

Thus, *Smith* compels the conclusion that the alleged collection of metadata records about Plaintiff's telephone calls does not constitute a search for purposes of the Fourth Amendment, because she has no reasonable expectation of privacy in the information those records contain.

2. Even if Plaintiff Had a Protectable Privacy Interest in Telephony Metadata, She Has Not Shown an Infringement of Her Privacy Through Review of Metadata Pertaining to Her Calls.

Even if the Court were to find that, contrary to *Smith*, Plaintiff has a reasonable expectation of privacy in metadata allegedly collected about her phone calls, she points to no invasion of that interest that would rise to the level of a Fourth Amendment search.

Call detail records are not "searched" in a constitutional sense every time an electronic query of the database is performed to determine which identifiers a "seed" has been in contact

[8] Plaintiff's effort to distinguish between the collection of data at the phone company's central offices in *Smith* and the collection of telephony metadata from telecommunications service providers here, Pl.'s PI Br. at 14, does not succeed. Both cases involve situations where the provider makes available to the government information that the provider already acquires and maintains for its own business purposes, irrespective of any interest the government may have in the information. Plaintiffs' reliance on *Ferguson v. Charleston*, 532 U.S. 67 (2001), for the proposition that "[w]hen the government does not actually collect the information, it raises serious Fourth Amendment concerns," Pl.'s PI Br. at 14, is also difficult to fathom. *Ferguson* involved warrantless and nonconsensual drug tests of pregnant women conducted for criminal investigatory purposes by a *state* hospital. Hence, it was the government collecting the information at issue, as the Court held. 532 U.S. at 76. Moreover, it was undisputed that the drug tests were searches, *id.*—the issue in the case was the reasonableness of the searches—distinguishing it from the question at bar.

with, as Plaintiff asserts. The only information made available for human review in response to such a query are the identifiers (and related metadata) that have been in direct or indirect contact with the terrorist identifier used to initiate the query. The NSA analyst receives no information about the calls of an individual whose identifiers have not had contact with the seed, except that the individual has not communicated with the suspected terrorist operative associated with the seed identifier. *See* Shea Decl. ¶¶ 20-26. The query process is analogous, in Fourth Amendment terms, to a canine sniff to "the presence or absence of narcotics" in a person's luggage, which "does not expose noncontraband items that otherwise would remain hidden from public view, as does … an officer's rummaging through the [luggage's] contents." *Place*, 462 U.S. at 707 (holding that exposing luggage to a canine sniff is not a search). *See also Jacobsen*, 466 U.S. at 123 ("A chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy"). The court's conclusion to the contrary in *Klayman*, 2013 WL 6571596, at *16, was thus both legally and factually unsound.[9]

[9] It is well settled, also, that the Government's seizure of an item, without inspection of its contents, "does not compromise the interest in preserving the privacy of [the] contents." *See Horton v. California*, 496 U.S. 128, 142 n.11 (1990) (and cases cited therein). This principle has been applied to items such as personal luggage, *see Texas v. Brown*, 460 U.S. 730, 748-49 (1983) (Stevens, J. concurring); first-class mail, *see United States v. VanLeeuwen*, 397 U.S. 249, 252-53 (1970) (defendant's interest in the privacy of his detained first-class mail "was not disturbed or invaded" until the Government searched it); packages brought aboard airplanes, *see United States v. Licata*, 761 F.2d 537, 541 (9th Cir. 1985) (seizure of package "affects only the owner's possessory interests and not the privacy interests vested in the contents"); and in recent years, computers and the files they contain. *See, e.g.*, *United States v. Clutter*, 674 F.3d 980, 984 (8th Cir. 2012) (seizure of computers, found later to contain child pornography, did not implicate privacy interests at time of seizure); *United States v. Bradley*, 488 F. App'x 99, 104 (6th Cir. 2012) (courts have analogized computers to closed containers for Fourth Amendment analysis); *United States v. Lucas*, 2008 WL 4858197, at *8 (W.D. Ky. Sept. 23, 2008) (same); *United States v. Costin*, 2006 WL 2522377, at *7 n.7 (D. Conn. July 31, 2006). The same principle applies here: the NSA's collection of call-detail records under the telephony metadata program does not itself intrude upon any hypothetical privacy interest there may be in the information contained in those records, because that information is not subject to review by NSA analysts unless and until the records are responsive to a query of the database.

Because Plaintiff has not shown that information associated with any of her phone calls has been reviewed by analysts in response to queries of the bulk telephony metadata collected by the NSA, she cannot maintain that NSA queries of the database intrude upon any putative expectation of privacy she claims to have in that information.

3. The Telephony Metadata Program Is Reasonable

Finally, even if the collection, querying, and review of bulk telephony metadata constituted a "search," the Fourth Amendment bars only "unreasonable" searches and seizures. The program at issue here is reasonable under the standard applied 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." *NTEU v. Von Raab*, 489 U.S. 656, 665-66 (1989). More specifically, the scope of the privacy interest and the character of the intrusion are balanced against the nature of the government interests to be furthered, the immediacy of the government's concerns regarding those interests, and the efficacy of the program in addressing those concerns. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 658, 660, 662-63 (1995).

The telephony metadata program clearly serves special governmental needs above and beyond normal law enforcement. The undisputed purpose of the telephony metadata program 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., United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322-23 (1972); *In re Sealed Case*, 310 F.3d 717, 746 (FISC-R 2002).

If, contrary to *Smith*, Plaintiff could be said to have any Fourth Amendment privacy interest that is implicated by the mere 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 review and dissemination of the metadata, that are 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 review of telephony metadata promote overriding public interests. The 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) ("[N]o 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) (Government interest in national security "is of the highest order of magnitude."); *ACLU*, 2013 WL 6819708, at *24. That interest cannot be as effectively achieved by requiring individualized suspicion to collect metadata, because such a requirement would not permit the type of historical analysis, contact-chaining, and timely identification of terrorist contacts that the broader collection enables. *See* Aug. 29 FISC Op. at 20-22; *ACLU*, 2013 WL 6819708, at *18. Imposing an individualized suspicion requirement on this program, is not only "impracticable" but may also be entirely infeasible. *Von Raab*, 489 U.S. at 665-66.

B. The Remaining Preliminary Injunction Factors Also Require Denial of Plaintiff's Motion

In addition to the fact that Plaintiff's Fourth Amendment claim has no prospect of success on the merits, Plaintiff cannot carry her burden on the remaining preliminary injunction factors: irreparable harm, the balance of the equities, and the public interest. First, Plaintiff claims that

the loss of her Fourth Amendment rights, "'for even minimal periods of time, unquestionably constitutes irreparable injury,'" Pl.'s PI Br. at 15 (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion)). But Plaintiff has failed to show a likelihood that her Fourth Amendment rights are in fact being denied, and so cannot "demonstrate that irreparable injury is *likely* in the absence of an injunction." *Winter*, 555 U.S. at 22 (emphasis in original); *see Battelle Energy All., Inc.*, 2013 WL 5818559, at *7. Otherwise, Plaintiff has not even alleged, and certainly not demonstrated, that she is suffering any consequences as a result of the telephony metadata program, much less injury so grave as to constitute irreparable harm.

Moreover, Plaintiff's delay in seeking a preliminary injunction also undermines her claim of irreparable harm. "Although delay by itself is not a determinative factor in whether the grant of interim relief is just and proper," *Miller v. California Pac. Med. Ctr.*, 991 F.2d 536, 544 (9th Cir. 1993) (internal quotation and alternations omitted), it is "relevant in determining whether relief is truly necessary." *Id.* Here, Plaintiff filed her original complaint on June 12, 2013 (ECF. No. 1), but then waited more than six months, until December 20, 2013, to seek preliminary injunctive relief. *See* Pl.'s PI Mot. This "long delay" between the filing of the complaint and the preliminary injunction "implies a lack of [both] urgency and irreparable harm." *Oakland Tribune, Inc. v. Chronicle Publ'g Co.*, 762 F.2d 1374, 1377 (9th Cir. 1985).

Second, the harm to Plaintiff if injunctive relief is denied is far outweighed by the harm to Defendants if it is granted. *See Winter*, 555 U.S. at 24. Complying with the injunction Plaintiff seeks would be extremely burdensome. NSA technical experts would have to develop the capability to segregate any metadata associated with Plaintiff's identifiers from the rest of the database, and also remove only her identifiers (and associated metadata) from each new batch of metadata received on a daily basis. *See* Shea Decl. ¶ 68. To design, build, test, and implement such a solution could require the hiring of additional personnel, take as long as six months, and,

if the injunction were to be lifted later, require additional resources to reverse the modifications made and re-integrate the data that had been set aside. *Id.* For her part, other than asserting that her Fourth Amendment rights are being violated (which they are not), Plaintiff points to no Government examination or dissemination of information about her or persons with whom she communicates, or any other impact the telephony metadata program has had on her. Under these circumstances, the balance of hardships tilts sharply against awarding preliminary relief.

Finally, the public interest would be disserved if a preliminary injunction were granted. Plaintiff invokes the principle that "[i]t is always in the public interest to prevent the violation of a party's constitutional rights," Pl.'s PI Br. at 16 (quoting *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012)), but no violation of Plaintiff's rights has been shown here. In contrast, the public interest in the telephony metadata program as a means of detecting and preventing intended terrorist attacks is a powerful one. *See Humanitarian Law Project v. Holder*, 130 S. Ct. 2705, 2724 (2010) ("the Government's interest in combating terrorism is an urgent objective of the highest order."); *Winter*, 555 U.S. at 24 (court must take into account an injunction's "consequent adverse impact on the public interest in national defense"). Here, NSA and FBI officials responsible for protecting the Nation against future terrorist attacks have affirmed that the program "is a valuable source of intelligence for the FBI that is relevant to FBI-authorized international terrorism investigations," Giacalone Decl. ¶ 22; *see* Shea Decl. ¶¶ 47-65. The Court should accord "great deference" to the professional judgment of these senior intelligence officials in such matters of national security. *See Winter*, 555 U.S. at 27. *See also ACLU*, 2013 WL 6819708, at *25 (finding that the "effectiveness of bulk telephony metadata collection cannot be seriously disputed," and that the public record of its successes "offer[s] ample justification" for the program). Following a recent review of intelligence programs, the President also stated his view that "it is important that the capability that this program is

designed to meet is preserved." President's Remarks at 5.[11] Thus, the public interest also weighs heavily in favor of Defendants, and Plaintiff's motion for preliminary relief must be denied.

III. PLAINTIFF'S AMENDED COMPLAINT SHOULD BE DISMISSED FOR LACK OF JURISDICTION AND FOR FAILURE TO STATE A CLAIM.

Not only must Plaintiff's motion for a preliminary injunction be denied, but, even if she had established her standing (which she has not) her amended complaint should be dismissed in part for lack of jurisdiction under Rule 12(b)(1) and in its entirety for failure to state a claim on which relief can be granted. To withstand a motion to dismiss under Rule 12(b)(6), a complaint must "contain 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), and not a mere "possibility or conceivability that a defendant has acted unlawfully." *Salameh v. Tarsadia Hotel*, 726 F.3d 1124, 1129 (9th Cir. 2013). To meet this standard, the "well-pleaded allegations" must allow "the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678-79. "Where a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief," *Salameh*, 726 F.3d at 1129 (quoting *Iqbal*, 556 U.S. at 678 internal quotation omitted). "[C]onclusory statements" and "bare assertions" of fact "are not

[11] The Court "should [also] give due weight to the serious consideration of the public interest in [the program] that has already been undertaken by the responsible [Government] officials." *Stormans, Inc. v. Selecky*, 586 F.3d 1109, 1140 (9th Cir. 2009); *see* President's Remarks, at 6 (directing Intelligence Community and Attorney General to develop options for a new approach to preserve the program's capabilities without the Government holding the data; ordering immediate implementation of new privacy protections; and pledging to consult with Congress and to seek authority for a new program as needed); Shea Decl. ¶¶ 37-38 (discussing implementation of transition ordered by the President); *see ACLU*, 2013 6819708, at *1 (noting the "robust discussions" about the program "underway across the nation, in Congress, and at the White House," and observing that "the question of whether th[e] program," while lawful, "should be conducted is for the other two coordinate branches of Government to decide").

entitled to the presumption of truth" and must be "discount[ed]" prior to "determining whether a claim is plausible." *Id.*[12]

The complaint in this case falls well short of *Iqbal*'s plausibility standard. Plaintiff asserts three causes of action: (1) that the telephony metadata program exceeds the authority granted by Section 215, (2) that the program violates the First Amendment, and (3) that the program violates the Fourth Amendment. Am. Compl. ¶¶ 25-27. Plaintiff's Fourth Amendment claim must be dismissed for the reasons discussed above. For the reasons below, Plaintiff's statutory claim should be dismissed for lack of jurisdiction and failure to state an actionable basis for relief. Plaintiff's First Amendment claim likewise fails to state a claim as a matter of law.

A. Congress Impliedly Precluded Judicial Review of Plaintiff's Statutory Claim.

Congress has impliedly precluded judicial review of the type of statutory claim Plaintiff asserts—that is, a claim for declaratory and injunctive relief, brought under the Administrative Procedure Act (APA), by a telephone subscriber alleging that the NSA's collection of telephony metadata, pursuant to a FISC order, exceeds the Government's authority under Section 215. *See* Am. Compl. ¶ 25. Because this claim is precluded, Plaintiff cannot rely on the waiver of sovereign immunity codified in the APA, 5 U.S.C. § 702, to supply the needed waiver for her 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 do any of the APA's provisions for judicial review, including APA § 702, apply where "statutes preclude judicial review" of a claim, as Section 215 clearly does here. *Id.* § 701(a)(1). Both courts to consider the question have concluded that review of the same statutory claim that Plaintiff seeks

[12] Defendants reserve the right to contest Plaintiff's allegations, and/or ability to prove her allegations without implicating protected state secrets, as may be necessary in further proceedings.

to present here is precluded by statute. *ACLU*, 2013 WL 6819708, at *9-13*; Klayman*, 2013 WL 6571596, at *9-12. Plaintiff's statutory claim must therefore be dismissed.[13]

"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); *see also FDIC v. Meyer*, 510 U.S. 471, 475 (1994) ("Absent a waiver, sovereign immunity shields the Federal Government and its agencies from suit."). It is further axiomatic that the Government's consent to suit "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 it does not "[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, echoing 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." *Id.* § 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

[13] Defendants assert no similar jurisdictional bar to Plaintiff's constitutional challenges to the telephony metadata program. Courts require a heightened showing of Congressional intent to preclude review of constitutional claims, so as "to avoid the serious constitutional question that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim." *Webster v. Doe*, 486 U.S. 592, 603 (1988). Defendants do not here maintain that FISA meets this heightened standard. *See ACLU*, 2013 WL 6819708, at *13.

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." 5 U.S.C. § 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.* at 349; *see Pottawatomi Indians*, 132 S. Ct. at 2213.

The courts in both *ACLU*, 2013 WL 6819708, at *9-13, and *Klayman*, 2013 WL 6571596, at *9-12, were presented with the same statutory challenge that Plaintiff attempts to raise here, and correctly held that those challenges were impliedly precluded by the USA PATRIOT Act. Two provisions of that Act are pertinent. First, section 223 of the Act, 18 U.S.C. § 2712, 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, not including Section 215, all of which involve

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).[14] Congress further stipulated that an action under section 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 Plaintiff 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. *ACLU*, 2013 WL 6819708, at *10-11; *Klayman*, 2013 WL 6571596, at *12 n.30. *See also Jewel v. NSA*, 2013 WL 3829405, at *12 (N.D. Cal. July 23, 2013) (section 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.").

Second, Section 215 forecloses the statutory claim for injunctive relief asserted here, by this type of plaintiff, in this forum. *ACLU*, 2013 WL 6819708, at *12-13; *Klayman*, 2013 WL 6571596, at *10-12. 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

[14] The enactment of section 223 of the USA PATRIOT Act in 2001 preceded enactment of 50 U.S.C. § 1861(h) in 2006. Congress has not since amended § 2712 to include violations of § 1861(h) as a basis for suit.

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, "section 215 does not provide for any person other than a recipient of an order to challenge [its] legality or otherwise participate in the process." *ACLU*, 2013 WL 6819708, at *12.

Congress chose this review process to ensure that meaningful judicial review of Section 215 orders is available while 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 recipient obviously knows of its existence and can challenge it in court."[15] Congress considered whether to extend a similar right of action to certain third parties (targets), but declined to do so because it would have been incompatible with the secrecy required for Section 215 orders.[16] 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). In creating this statutory

[15] *Implementation of the USA PATRIOT Act: Hrg Bef. the H. Subcomm. on Crime, Terrorism, and Homeland Security, Comm. on the Judiciary*, 109th Cong. at 65 (2005).

[16] *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).

framework, "Congress did not envision that third parties, such as [P]laintiff[], would even *know* about the existence of Section 1861 orders, much less challenge their legality under the statute." *Klayman*, 2013 WL 6571596, at *10. *See also ACLU*, 2013 WL 6819708, at *12 ("Section 215 does not just exclude a target from challenging an order, it precludes their participation in any way."); H.R. Rep. No. 109-174 at 128 (2005).

The fact that Plaintiff learned about the program she seeks 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. "It cannot possibly be that lawbreaking conduct by a government contractor that reveals state secrets—including the means and methods of intelligence gathering—could frustrate Congress's intent." *ACLU*, 2013 WL 6819708, at *13.

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," as both *ACLU* and *Klayman* expressly held.[17]

B. The NSA's Bulk Collection of Telephony Metadata Is Authorized Under Section 215.

Even if review of Plaintiff's statutory claim were not precluded, it should still be dismissed. The complaint does not state the basis of Plaintiff's statutory claim, but litigants in

[17] *See also 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 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).

other cases have contended that collection of bulk telephony metadata is not authorized by Section 215 because the records collected are not "relevant" to authorized national security investigations. *See, e.g.*, *ACLU*, 2013 WL 6819708, at *17; *Klayman*, 2013 WL 6571596, at *9. That argument was rejected in *ACLU* (the court in *Klayman* did not reach it), and if raised should be rejected here as well.

1. The NSA'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-six occasions that the Government satisfied this requirement, finding "reasonable grounds to believe" that the telephony metadata sought by the Government "are relevant to authorized FBI investigations to protect against international terrorism." Giacalone Decl. ¶¶ 6, 11; *see* Primary Order at 1; Aug. 29 FISC Op. at 11; Oct. 11, 2013, FISC Mem. at 3. The Court reached the same conclusion in *ACLU*, 2013 WL 6819708, at *16-18, and so, too, should this Court.

a. The bulk telephony metadata collected by the NSA 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 litigation, 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 and highly deferential standard of relevance 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 subpoena power conferred on administrative agencies affords them "access to virtually any material that might cast light on the allegations" at issue in an investigation, *EEOC v. Shell Oil Co.*, 466 U.S. 54, 68-69 (1984), and an agency's appraisal of relevancy to its investigation "must be accepted so long as it is not obviously wrong," *NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 193 (2d Cir. 2006) (internal quotation omitted); *FTC v. Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1992) (same). *See ACLU*, 2013 WL 6819708, at *17. In light of that basic understanding of relevance, courts in these contexts categorically authorize the production of entire repositories of records, even when any particular record is unlikely to bear directly on the matter being investigated, where reviewing 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. *See id.* at *18.[19]

[19] *See also 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 subpoenas for records of wire money transfers "involving hundreds of innocent people"); *Carrillo Huettel, LLP v. SEC*, 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011) (trust account data 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, 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").

Analogously, courts issue search warrants permitting officials 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); *United States v. Hill*, 459 F.3d 966, 975 (9th Cir. 2006)

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 requirement, *see* USA PATRIOT Act Improvement Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2006), and "mean[t] to incorporate [its] established meaning." *NLRB v. Amax Coal Co.*, 453 U.S. 322, 329 (1981). It was well recognized at the time that relevance was equivalent to 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).[20] Congress in fact described the items subject to production under Section 215 as including things obtainable by "a subpoena duces tecum issued by a court . . . in aid of a grand jury investigation." 50 U.S.C. § 1861(c)(2)(D). Underscoring that Section 215's standard of relevance should be at least as deferential as in these other contexts, Congress conditioned the Government's collection of business records on a showing, not of relevance, but of "*reasonable grounds to believe* that the [records] are relevant" to authorized counter-terrorism investigations. *Id*. § 1861(b)(2)(A) (emphasis added), (c)(1); *ACLU*, 2013 WL 6819708, at *17.

Of course, the case law in these contexts does not involve data collection on the scale of the telephony metadata program. But here, 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). Ordinarily, criminal or administrative inquiries focus retrospectively on specific crimes or violations that have already occurred and the persons

---

(recognizing that "blanket seizure" of the defendant's entire computer system, with subsequent review, may be permissible).

[20] *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).

known or suspected to have committed them. In contrast, the purpose of counter-terrorism investigations 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 intended targets, and means of attack. *See CIA v. Sims*, 471 U.S. 159, 171 (1985) ("foreign intelligence consists of securing all possible data pertaining to . . . the national defense …"); *U.S. Dist. Court (Keith)*, 407 U.S. at 322-23; Giacalone Decl. ¶¶ 17-18. Thus, relevance in this context must take into account the far-reaching information gathering required to shed light on terrorist groups, their composition, objectives, and capacity for carrying out their plans. *ACLU*, 2013 WL 6819708, at *18.

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 id.*; H.R. Rep. No. 109-174(1) at 129 (statement of Rep. Lungren); 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 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. Giacalone Decl. ¶¶ 8-9, 17-26; Shea Decl. ¶¶ 47-49; *see* Aug. 29 FISC Op. at 20. Targeted tools of investigation that do not involve bulk collection 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 group, where in the data the terrorists' communications can be found. Giacalone Decl. ¶¶ 9, 27-29; Shea Decl. ¶¶ 60-65. Absent the creation of an historical repository of information that aggregation of bulk data allows, it may not be feasible for the NSA to identify chains of communications among known and unknown terrorist operatives that cross different time periods and provider networks. Giacalone Decl. ¶¶ 9, 27-29; Shea Decl. ¶ 61; *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. As the FISC stated, and the Court in *ACLU* agreed,

> [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.

Id. at 18; *see also* Oct. 11 FISC Mem. at 3; *accord ACLU*, 2013 WL 6819708, at *18 (armed with the metadata, the NSA can detect connections with foreign terrorist organizations that it might otherwise never be able to find).[21]

[21] In another recently released FISC opinion, the FISC concluded, for like reasons, that bulk collection of Internet metadata satisfied the relevance requirement of FISA's pen/trap provision, 50 U.S.C. § 1842. *[Redacted]* (Exh. H), Opinion and Order at 47-49; *see id.* at 40-46.

b. Congress legislatively ratified the collection of bulk telephony metadata records under Section 215

The conclusion that bulk telephony metadata are "relevant" within the meaning of Section 215 is reinforced, as the FISC and the *ACLU* court recently recognized, by Congress's extension of Section 215's authorization in 2010 and 2011, without substantive change, after receiving notice that the Executive Branch had interpreted Section 215 to permit, and the FICA had authorized, the bulk collection of telephony metadata. Aug. 29 FISC Op. at 23-28; Oct. 11 FISC Mem. at 3; *ACLU*, 2013 WL 6819708, at *15-16. In December 2009, a classified briefing paper, explaining that the Government had interpreted Section 215 to permit the bulk collection of telephony metadata, and that the FISC had authorized the collection, 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."[22] The classified use of this authority has also been briefed numerous times over the years to the Senate and House Intelligence and Judiciary Committees.[23]

---

[22] *See* Letter from Ronald Weich to the Hon. Silvestre Reyes (Dec. 14, 2009) (Exh. I); Report on the [NSA's] Bulk collection Programs for USA-PATRIOT Act Reauthorization (Exh. J). 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. K); Letter from Rep. Reyes to Colleagues (Feb. 24, 2010) (Exh. L); *see also* 156 Cong. Rec. H838 (daily ed. Feb. 25, 2010) (statement of Rep. Hastings); 156 Cong. Rec. S2109 (daily ed. Mar. 25, 2010) (statement of Sen. Wyden). An updated version of the briefing paper, *see* 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. N); Letter from Ronald Weich to the Hon. Mike Rogers and the Hon. C.A. Dutch Ruppersberger (Feb. 2, 2011) (Exh. O). 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. P).

[23] *See* Press Release of Sen. Select Comm. on Intelligence (June 6, 2013) (Exh. Q)); *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. R).

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.[24] "'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)). Both the *ACLU* court and the FISC found that to be the case here, where Congress had actual and repeated notice of the Executive Branch's administrative construction of Section 215 over a period of years. *ACLU*, 2013 WL 6819708, at *16 (finding "that Congress ratified section 215 as interpreted by the Executive Branch and the FISC, when it reauthorized FISA."); Aug. 29, 2013 FISC Op. at 27 (finding "well-supported" factual basis for presuming that "Congress intended to ratify Section 215 as applied by this Court"). 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. Plaintiff's statutory claim should therefore be dismissed.

C. Plaintiff's First Amendment Claim Also Fails as a Matter of Law

1. Plaintiff Has Failed to Allege Any Direct or Indirect Burden on Her Freedom of Speech or Association

Plaintiff's amended complaint should also be dismissed so far as it purports to state a First Amendment claim. *See* Am. Compl. ¶ 26. Plaintiff makes no allegation, well-pleaded or otherwise, that her expressive or associational activities are burdened or chilled in any way by operation of the telephony metadata program. In the absence of plausible allegations that the program substantially burdens Plaintiff's freedom of speech or association, her First Amendment claim is deficient as a matter of law. *See, e.g.*, *United States v. Gering*, 716 F.2d 615, 620 (9th

[24] 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.

Cir. 1983) (rejecting defendant's First Amendment challenge to use of targeted "mail covers" where defendant made no showing of "particular detrimental effect" on his associational rights) (citing *United States v. Choate*, 576 F.2d 165, 181 (9th Cir. 1978)); *see also United States v. Mayer*, 503 F.3d 748, 749 (9th Cir. 2007) (similar); *ACLU*, 2013 WL 6819708 at *24 ("[B]ulk metadata collection does not burden First Amendment rights substantially.").

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

Plaintiff's First Amendment claim also fails for the reason that good-faith investigations carried out for purposes other than to deter or punish free speech or association do not violate the First Amendment. Recognizing the need to accommodate the Government's interests where prevention of crime, or, even more imperatively, potential threats to national security, are concerned, *see ACLU Found. v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991), 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 v. Tatum*, 408 U.S. 1, 11 (1972); *United States v. Mayer*, 503 F.3d 740, 751-53 (9th Cir. 2007). Thus, the law is clear that governmental investigative activities conducted in good faith and not "for the purpose of abridging first amendment freedoms" do not violate the First Amendment. *Mayer*, 503 F.3d at 751 (internal quotation omitted) (quoting *United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989)); *Reporters Comm.*, 593 F.2d at 1051-53.

Here, Plaintiff does not allege that the telephony metadata program has any objective other than furthering the compelling national interest in identifying and tracking terrorist operatives and ultimately thwarting terrorist attacks. The complaint certainly contains no

allegations from which it could plausibly be concluded that the program is aimed at curtailing any First Amendment expressive or associational activities. *See Mayer*, 503 F.3d at 752. To the contrary, her allegations regarding the FISC-authorized breadth of the collection, Am. Compl. ¶¶ 15-17, highlight the fact that it is undertaken without targeting Plaintiff or any other persons, and without reference to anyone's conduct protected by the First Amendment. Indeed, numerous safeguards built into the program prevent the Government from collecting or using the data for purposes forbidden by the First Amendment.[25]

Furthermore, as explained *supra*, at 7, the metadata collected do not reveal Plaintiff's name or address or those of anyone with whom she speaks, and, regardless, Plaintiff makes no allegation that metadata related to her communications have ever been reviewed by NSA analysts for any purpose, whether as the results of queries based on the "reasonable, articulable suspicion" standard, or otherwise. "Fear that telephony metadata relating to [Plaintiff] [may] be queried or reviewed or further investigated . . . is insufficient to . . . establish a violation of an individual's First Amendment rights." *ACLU*, 2013 WL 6819708, at *24.

Thus, Plaintiff has failed to state a First Amendment claim that plausibly gives rise to an entitlement to relief. *Iqbal*, 556 U.S. at 678-79. The amended complaint must be dismissed.

CONCLUSION

For the reasons stated above, Plaintiff's motion for a preliminary injunction should be denied, and this case should be dismissed.

[25] *See* Primary Order at 8-9 (requiring NSA General Counsel's Office 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").

Dated: January 25, 2014

Respectfully submitted,

WENDY J. OLSON, Idaho Bar No. 7634
United States Attorney

SYRENA C. HARGROVE, Idaho Bar No. 6213
Assistant United States Attorney

District Of Idaho
Washington Group Plaza IV
800 E. Park Boulevard, Suite 600
Boise, ID 83712-9903
Telephone: (208) 334-1211
Facsimile: (208) 334-1414
Syrena.Hargrove@usdoj.gov

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

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

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

RODNEY PATTON
Trial Attorney

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

Counsel for Defendants