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
RODNEY PATTON
Trial Attorneys
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

UNITED STATES DISTRICT COURT
DISTRICT OF IDAHO

ANNA J. SMITH, Plaintiff, v. BARACK OBAMA, President of the United States, *et al.*, Defendants.	No. 2:13-cv-00257-BLW **REPLY IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS**

INTRODUCTION

Plaintiff concedes that her claims that the telephony metadata program violates the First Amendment and applicable statutory law "may be dismissed." Plaintiff's Combined Reply in Support of Plaintiff's Motion for Preliminary Injunction and Objection to Defendants' Motion to Dismiss (Pl.'s Reply & Obj.) (ECF No. 17) at 14. Accordingly, Defendants' motion to dismiss Plaintiff's first and second causes of action, Amended Complaint ¶¶ 25-26, should be granted. *See* Memorandum in Opposition to Plaintiff's Motion for a Preliminary Injunction and in Support of Defendants' Motion to Dismiss (Defs.' Br.) (ECF No. 15) at 30-43.

Plaintiff's remaining claim, that the program violates the Fourth Amendment, also should be dismissed. Plaintiff does not have standing to assert that claim because she can only speculate that the Government collects metadata associated with her calls; and, even if the Government did collect that metadata, her concession that she cannot show that the Government has reviewed that data, *see* Pl.'s Reply & Obj. at 5, 7, 12, means that she has not shown an invasion of a legally protected interest.

Moreover, even if Plaintiff could demonstrate that she has standing, her Fourth Amendment claim fails as a matter of law. The collection of telephony metadata does not constitute a search because, as the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), subscribers do not have a reasonable expectation of privacy in telephony metadata associated with their calls. Plaintiff's repeated attempts to distinguish *Smith* are unavailing.

Additionally, even if there is a reasonable expectation of privacy in telephony metadata, Plaintiff has not plausibly alleged that any putative expectation of privacy is compromised merely by electronic queries of NSA's database with selectors associated with terrorism. And, finally, even if those queries constituted searches, Plaintiff has not addressed, much less rebutted,

the Government's showing that the program complies with the Fourth Amendment because it satisfies the special needs doctrine.

As a result, Plaintiff's remaining claim should also be dismissed for lack of subject matter jurisdiction, or, alternatively, for failure to state a claim.

ARGUMENT

I. PLAINTIFF DOES NOT HAVE STANDING TO CHALLENGE THE TELEPHONY METADATA PROGRAM.

Plaintiff concedes that "[o]nly the Government knows whether it is collecting Plaintiff's phone records," Pl.'s Reply & Obj. at 5,[1] but she urges this Court nevertheless to infer that the Government is doing so based on statements in the President's recent speech regarding NSA intelligence programs, speculation by the court in another case involving a challenge to the legality of the telephony metadata program, and the Government's official acknowledgments regarding the existence of, and certain details about, the telephony metadata program. *Id.* at 6. There is no basis in these materials for the Court to make such an inference. Plaintiff points to no specific passage of the President's speech on January 17, 2014, to support her contention that "the phone records of nearly all Americans are being collected and stored." *Id.* And, contrary to Plaintiff's assertion, the Government has not "for all intents and purposes admitted" that it collects telephony metadata associated with Plaintiff's calls. *See id.* at 6-7.[2] The Government

[1] Plaintiff observes that "the Government is in the best position to tell the Court that it is *not* collecting Plaintiff's phone records" and calls its failure to do so a "lack of candor." Pl.'s Reply & Obj. at 5. Not so. As the Supreme Court observed, it is Plaintiff's "burden to prove [her] standing by pointing to specific facts, not the Government's burden to disprove standing by revealing details" of still-classified facts. *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1149 n.4 (2013) (citation omitted).

[2] Plaintiff surmises that Defendants' use of the term "telephony metadata" is "likely intended to downplay the privacy concerns" in what she calls "her 'phone records.'" Pl.'s Reply & Obj. at 4 n.1. Any data collected, however, are indisputably business records created and maintained by the pertinent telecommunications providers for their own business purposes. *See,*

has acknowledged the existence of the telephony metadata program, and confirmed that it involves the collection and aggregation of data from multiple telecommunications service providers, *see* Defs.' Br. at 13; Pl.'s Reply & Obj. at 6, but has not disclosed the specific scope of that collection or whether or not Plaintiff's carrier, Verizon Wireless (or her former carrier, AT&T), participates in the Section 215 telephony metadata program. *See* Defs.' Br. at 12-13.

Plaintiff also describes as "facts" supporting her standing a chain of speculative assumptions made by the court in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), upon which Plaintiff seeks to rely. *See* Pl.'s Reply & Obj. at 6. As an initial matter, even if the *Klayman* court's speculation were taken as findings of fact, "judicial fact[-] findings" from another court's decision, offered to "prove the truth of those findings," are inadmissible hearsay, *United States v. Sine*, 493 F.3d 1021, 1036 (9th Cir. 2007), and thus cannot be used as a "short cut" to bring those facts before this Court, *see id.* at 1031-32.

Moreover, the assumptions from *Klayman* upon which Plaintiff seeks to rely are not supported either by the record here or before the *Klayman* court. Specifically, Plaintiff relies upon the *Klayman* court's characterization of the Government's description of the metadata program as one that "can function *only*" through the "creat[ion of] a *comprehensive* metadata database that serves as a potentially valuable tool in combating terrorism." *Klayman*, 957 F. Supp. 2d at 21 (emphasis in original); *see also* Pl.'s Reply & Obj. at 6. The Government has stated—to the *Klayman* court and to this Court—that the telephony metadata program is an important counterterrorism tool, Pl.'s Reply & Obj. at 6; Defs.' Br. at 1, 3, 29, and that this tool would not have the same capability if only communication records of known terrorists were collected. Defs.' Br. at 13. The Government has also acknowledged that the program is broad in scope and involves the aggregation of an historical repository of data collected from more than

---

e.g., *Smith*, 442 U.S. at 742-43; *ACLU v. Clapper*, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013).

one provider. *Id.* But the Government has not represented that the utility of the program depends on the existence of a "complete database of all phone records." Pl.'s Reply & Obj. at 6; *see also* Defs.' Br. at 12-14. Indeed, to the contrary here, Defendants have explained (with the only competent evidence of record on this point) that the program "has never captured information on all (or virtually all) calls made and/or received in the U.S." *See* Shea Decl. ¶ 17; *see also* Defs.' Br. at 13 (citing Aug. 29 FISC Op. at 4 n.5 ("[P]roduction of all call details records of all persons in the United States has never occurred under this program.").

Proceeding from its own assumption about the scope of the program, the *Klayman* court surmised—and Plaintiff asks this Court to do the same—that "the NSA *must* have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States." *Klayman*, 957 F. Supp. 2d at *27 (emphasis in original); Pl.s' Reply & Obj. at 6. But that was (and is) no more than speculation because it is not based on any actual confirmation by the Government or specific evidence in the record, and this Court should decline Plaintiff's invitation to speculate about still classified matters in order to infer the existence of standing. At bottom, Plaintiff is relying on her own conjecture about whether her carrier is a participant in the program, and such speculation cannot substitute for the "specific facts" that must be shown in order to establish standing. *See Amnesty Int'l, USA*, 133 S. Ct. at 1147-48 (speculation that an injury in fact has or will occur is insufficient to confer standing).

Not only are Plaintiff's claims about the scope of the metadata collection speculative and insufficient to establish standing, but they are beside the point. Even if Plaintiff could show that metadata associated with her calls have been collected, she still would not establish her standing to challenge the program. Given that Plaintiff concedes, as she must (Defs.' Br. at 14-15), that she "cannot prove that her metadata has been 'reviewed' by the NSA," Pl.'s Reply & Obj. at 7, she nevertheless argues (Pl.'s Reply & Obj. at 7)—once again without citation—that mere

querying of the database by the NSA (using identifiers that are reasonably suspected of association with specified terrorist organization) constitutes "a search of Plaintiff's call records" and thus confers on her "standing to challenge this search." Pl.'s Reply Br. at 7. Absent some indication that NSA has actually reviewed records with metadata associated with her calls, Plaintiff cannot show that an electronic query of a database under the "reasonable, articulable suspicion" standard constitutes an "*invasion* of a legally protected interest," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (emphasis added), and Plaintiff has failed to even address the substantial authority Defendants cite on this point. *See* Defs.' Br. at 15 & n.4, 24-26 (citing *inter alia*, *Horton v. California*, 496 U.S. 128, 142 n.11 (1990) (government's acquisition of an item without examining its contents "does not compromise the interest in preserving the privacy of its contents")).

For these reasons and those set forth in Defendants' initial brief, this Court should dismiss Plaintiff's remaining Fourth Amendment claim for lack of subject matter jurisdiction.

II. PLAINTIFF'S CLAIM THAT THE TELEPHONY METADATA PROGRAM VIOLATES HER FOURTH AMENDMENT RIGHTS FAILS AS A MATTER OF LAW.

Assuming, *arguendo*, Plaintiff could establish her standing, her opposition brief nonetheless fails to show that, as a matter of law, individuals have a reasonable expectation of privacy in telephony metadata in a provider's records, as would be necessary for there to be a search under the Fourth Amendment, or that the NSA's electronic querying of the metadata, without more, constitutes an infringement on any putative expectation of privacy that could constitute a search in violation of her Fourth Amendment rights. Plaintiff's opposition brief also fails to address a separate point made in Defendant's initial brief—that, even if the program involved a search, it would be reasonable given the important national security interests the program serves and the minimal extent of any intrusion on individual privacy. *See* Defs.' Br. at

26-27; *see also* U.S. Const. amend. IV (prohibiting only "unreasonable searches and seizures"). Plaintiff's Fourth Amendment claim could also be dismissed on this basis alone.

A. There Is No Reasonable Expectation of Privacy In Telephony Metadata and There Has Therefore Been No Search for Purposes of the Fourth Amendment.

As in her initial brief, Plaintiff again attempts to distinguish *Smith* from the case at bar by relying on distinctions without a difference. *See* Pl.'s Reply & Obj. at 9-13. None of the distinctions Plaintiff attempts to draw are material to the reasoning of *Smith*—*i.e.*, that individuals have no reasonable expectation of privacy in the telephone numbers they dial because they voluntarily turn that information over to a third party (a telecommunications provider), thus assuming the risk that the company will turn them over to the government. *Smith*, 442 U.S. at 743-44.

First, Plaintiff's argument—that the "collection [of] call records was a 'search' in *Smith*, and it is a 'search' here," Pl.'s Reply & Obj. at 9—is wrong on both counts. The court in *Smith* clearly found that the person whose phone records were collected "in all probability entertained no actual expectation of privacy" in telephony metadata, or, "even if he did, his expectation was not 'legitimate,'" and then held that "the installation and use of a pen register, consequently, *was not a 'search'*" under the Fourth Amendment. *Smith*, 442 U.S. at 746 (emphasis added). The same conclusion applies here.

Second, while conceding that Fourth Amendment rights are personal in nature, Plaintiff nonetheless argues that the "scope of the Government's dragnet" search here distinguishes *Smith*, where only one person was targeted, Pl.'s Reply & Obj. at 11. Plaintiff previously raised this argument, Pl.'s PI Mem. at 14-15, and Defendants' response remains that the collection of metadata does not gain Fourth Amendment protection simply by virtue of the number of people whose data is collected. *See* Defs.' Br. at 21 (citing, *inter alia*, *ACLU*, 959 F. Supp. 2d at 752

("The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search.")).[3]

Third, Plaintiff reasons that the retention of telephony metadata here makes this case much less like *Smith* and more like *United States v. Jones*, 132 S. Ct. 945 (2012). *See* Pl.'s Reply & Obj. at 11. According to Plaintiff, the GPS device in *Jones* was attached to the suspect's car for four weeks and was thus "found to violate the reasonable expectation of privacy." *Id.* (citing Justice Sotomayor's concurrence). Again, Plaintiff is wrong. The Court in *Jones* decided that the use of a GPS device attached to a suspect's vehicle was a "classic trespassory search," and expressly disclaimed reliance on the duration of the monitoring (a factor on which the court below had relied),[4] as a basis for concluding that a search had occurred. *See Jones*, 132 S. Ct. at 954; *id.* at 955 (Sotomayor, J., concurring) ("When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principal suffices to decide this case."); *see also* Defs.' Br. at 23. And, as Defendants have explained, the concerns expressed in Justice Sotomayor's concurrence in *Jones* about GPS monitoring over an extended time revealing a wealth of information about a person's life, are not applicable here where the telephony metadata provided to the NSA contains no identifying information and the NSA is barred from searching for or reviewing such information outside the

[3] Relatedly, Plaintiff argues that "the scope of the search certainly goes to its reasonableness and distinguishes *Smith* from this case." Pl.'s Reply & Obj. at 10. But *Smith* dealt not with the reasonableness of a search but with "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment" in the first instance. *Smith*, 442 U.S. at 736.

[4] *See United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

confines of a query based on reasonable articulable suspicion to believe a phone number is associated with a foreign terrorist organization. *See* Defs.' Br. at 23.[5]

Fourth, Plaintiff also tries to distinguish *Smith* on the ground that the metadata collected here contains additional information that was not collected by the pen register in *Smith*. *See* Pl.'s Reply & Obj. at 12-13. But any such differences are not material to the constitutional issue at hand because, as in *Smith*, Plaintiff either turns over the pertinent information voluntarily to her telecommunications provider or it is generated by the provider itself. In either case, she does not have a reasonable expectation of privacy in the data. *See* Defs.' Br. at 20-21, 24; *see also Smith*, 442 U.S. at 742-44 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

Finally, Plaintiff's argument that *Smith* is inapplicable "in the 21st century" (*see* Pl.'s Obj. & Reply at 9-11) is demonstrably wrong, as well as an improper basis to reject controlling Supreme Court precedent. *See* Defs.' Br. at 22-23. Declining to take on the burgeoning case law cited in Defendants' initial brief—which demonstrate that courts, including the Ninth Circuit, continue to apply *Smith* and the third-party doctrine in the full bloom of the digital age, *see* Defs.' Br. at 19-21 & n.6[6]—Plaintiff chooses instead to distinguish a single case, *United States v.*

---

[5] Plaintiff takes issue with Defendants' argument (Defs.' Br. at 21-22) that the investigative activity was more invasive for the criminal defendant in *Smith* than the intelligence gathering activity here could be for Plaintiff, even presuming that metadata associated with her calls is actually collected. *See* Pl.'s Reply & Obj. at 11-12. Plaintiff does not, however, explain how law enforcement officers poring over the data related to the criminal defendant's calls in *Smith*, or prosecutors using that information to prosecute the defendant in *Smith*, is less invasive than the facts presented here, where Plaintiff concedes that "it may be true that a real person has never reviewed Plaintiff's call logs." *Id.* at 12.

[6] *See also, e.g.*, *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation because it is voluntarily conveyed to third parties.") (internal quotations omitted); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (same); *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (Internet subscriber information); *United States v. Qing Li*, 2008 WL 789899, at *4-5 (S.D. Cal. Mar. 20, 2008) (IP

Reed, 575 F.3d 900 (9th Cir. 2009), cited by Defendants, *see* Defs.' Br. at 20, and Pl.'s Reply & Obj. at 10-11. Plaintiff asserts that *Reed* is distinguishable from this case because *Reed* involved a "federal wiretap order." *Id.* That again is a distinction that is immaterial to the question at hand. While *Reed* did indeed involve a federal wiretap order to obtain the content of telephone conversations, *Reed*, 575 F.3d at 905, 915, the order "also authorized the use of a pen register and trap and trace device" that "directed the telephone company to provide the Government" with call data about "call origination, length, and time of call." *Id.* at 914. Here, the Foreign Intelligence Surveillance Act (FISA) Court issues an order, upon application by the FBI, directing a telecommunications provider to produce telephony metadata to the NSA. *See* Defs.' Br. at 5-9. And, just as in *Reed*, "there is no Fourth Amendment 'expectation of privacy'" in that collected telephony metadata. *Reed*, 575 F.3d at 914.[7]

B. Even if Plaintiff Could Show that She Had a Reasonable Expectation of Privacy in Telephony Metadata, She Has Not Plausibly Alleged That the Government Has Intruded Upon that Expectation.

Plaintiff has not alleged—much less plausibly alleged—that the NSA has ever reviewed telephony metadata associated with her calls and, indeed, concedes that an NSA analyst may never have reviewed her call records. Pl.'s Reply & Obj. at 12. In these circumstances, her

---

log-in histories and addressing information); *In re Application of the United States*, 830 F. Supp. 2d 114, 133-38 (E.D. Va. 2011) (Internet Protocol addresses); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (Internet subscriber information).

[7] Plaintiff asserts that the *Reed* court's holding, that collecting telephony metadata does not implicate the Fourth Amendment, "is dicta." Pl.'s Reply & Obj. at 10. She provides no explanation or citation why that should be so. Curiously, having just labeled the holding "dicta," Plaintiff also asserts that *Reed* is "helpful because it supports the conclusion that the collection of phone records is a 'search.'" *Id.* at 10-11. The court's finding that "there is no Fourth Amendment 'expectation of privacy,'" in collected telephony metadata, *Reed*, 575 F.3d at 914, and therefore no search, contradicts that assertion. Finally, Plaintiff observes that the *Reed* case "does not address whether such a search is reasonable outside of a criminal investigation," Pl.'s Reply & Obj. at 11, but that undoubtedly follows because the court in *Reed* held that no search involving metadata occurred in the first instance.

allegation of a Fourth Amendment violation necessarily fails, because, even if Plaintiff had a reasonable expectation of privacy in metadata about her telephone calls within a provider's records, she cannot show that an infringement on that expectation has occurred if metadata pertaining to her calls are not reviewed by NSA analysts (or anyone else) pursuant to queries made under the "reasonable, articulable suspicion" standard.

Recognizing this shortcoming, Plaintiff claims, without citing any authority, that every electronic query of the database under the "reasonable, articulable suspicion" standard constitutes a search. *See* Pl.'s Reply & Obj. at 12. Her assertion, however, does not address the point (or the supporting case law) that collection alone of call-detail records does not compromise a putative expectation of privacy in the data the records contain—and thus does not constitute a search—unless the contents of the records are reviewed. *See* Defs.' Br. at 24-26 (citing, *inter alia*, *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); *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")).[8]

Alternatively, Plaintiff claims that because the Government has the ability to store these records and, at some later undefined time, "mine them for information," there is a "real threat of a violation of Plaintiff's Fourth Amendment rights." Pl.'s Reply & Obj. at 12. But the statutorily

[8] In finding that the NSA's automated querying process constitutes a search, *see Klayman*, 957 F. Supp. 2d at 29, the *Klayman* court compared "hop one" of the process of "querying a foreign number" in the database to a person "entering a library and trying to find every book that cites" a particular book "as a source" because the "only way to know" that would be to "open every book in the library." *Id.* But one difference among many between the electronic querying process in the Section 215 program and the person in the *Klayman* court's analogy is that a NSA analyst does not review (or receive) information that is not responsive to the query term, *see* Defs.' Br. at 7, whereas the person in the library analogy must read every book in the library to determine whether it contains citations to the original book.

required minimization requirements imposed by the FISA Court (FISC) preclude the Government from "mining" the data in the manner Plaintiff fears, as does an extensive regime of internal Executive Branch and FISC oversight to ensure compliance with those requirements. *See* Defs.' Br. at 3-9. Accordingly, Plaintiff's concerns that her records, if collected, may nonetheless later be "mined" for her personal data is an insufficient basis to establish her standing to assert a Fourth Amendment claim, much less to plausibly allege that a such a "mining" violation has occurred. *See Amnesty Int'l, USA*, 133 S. Ct. at 1147 (no standing when injury asserted is not "certainly impending"); *City of Los Angeles v. Lyons*, 461 U.S. 95, 102, 105-06 (1983) (no standing for plaintiff to seek injunctive relief when he could not show he would likely be subject to alleged "chokehold" policy in the future).

CONCLUSION

Plaintiff has conceded that her first and second claims for relief should be dismissed. For the reasons stated above and in Defendants' motion, Plaintiff's Fourth Amendment claim should be dismissed as well.

Dated: March 14, 2014

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

Respectfully submitted,

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