PETER J. SMITH IV, ISB 6997
Lukins & Annis, P.S.
601 E. Front Avenue, Suite 502
Coeur d'Alene, ID 83814
Phone: 208-667-0517
Fax: 208-664-4125
Email: psmith@lukins.com

LUCAS T. MALEK, ISB 8610
Luke Malek, Attorney at Law, PLLC
721 N 8th Street
Coeur d'Alene, ID 83814
Phone: 208-661-3881
Email: Luke_Malek@hotmail.com

Attorneys for the Plaintiff ANNA J. SMITH

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

ANNA J. SMITH,

Plaintiff,

vs.

BARACK H. OBAMA, in his official capacity as President of the United States of America; JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

CASE NO. 2:13-cv-00257

PLAINTIFF'S COMBINED REPLY IN SUPPORT OF PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION AND OBJECTION TO DEFENDANTS' MOTION TO DISMISS

Table of Contents

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

> *It is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power, it is dependent on the law to constrain those in power.*

President Obama, January 17, 2014, Exhibit "G" to Declaration of James J. Gilligan filed January 24, 2014 (Doc 15-1) ("Gilligan Decl.").

The Government's response to Plaintiff's challenge of the collection of her phone records revealing who she calls, when she calls them, who calls her and how long she talks may be paraphrased as:

> *Trust us. We have "minimization procedures" that "strictly limit access to and review of metadata, and limit dissemination of information derived from the data, to valid counter-terrorism purposes."*

Memorandum in Opposition to Plaintiff's Motion for Preliminary Injunction and in Support of Defendants' Motion to Dismiss ("Dfs.' Opp. Br.") at 6.

As President Obama eloquently stated, "trust us" is not an answer that passes Constitutional muster. The question is whether the collection and query of Plaintiff's call records violates the Fourth Amendment.[1] Plaintiff is not asking this Court to find the Government is not trustworthy. Rather, Plaintiff is asking whether the law constrains the Government's power regardless of whether it is trustworthy or not. Plaintiff urges this Court to find that (1) she has

[1] The Government refers to the collection of Plaintiff's phone records as the collection of "telephony metadata." The use of this phrase is likely intended to downplay the privacy concerns. Plaintiff will refer to this information as her "phone records." Phone records that show who she called, who called her, when and how long they talked.

standing to challenge the Government's collection, retention and searching of her phone records; and (2) the Government's collection, retention and searching of her phone records likely violates a reasonable expectation of privacy protected by the Fourth Amendment.

ARGUMENT

1. PLAINTIFF HAS STANDING TO CHALLENGE THE GOVERNMENT'S COLLECTION OF HER PHONE RECORDS.

The Government argues that Plaintiff "failed to allege or demonstrate an injury meeting Article III's standards." Dfs.' Opp. Br. at 12. The Government first argues that Plaintiff only has a "speculative fear" show that her phone records have been collected. *Id.* Second, the Government argues that Plaintiff can not show that her phone records have been actually reviewed by the NSA. *Id.* 14. Each argument will be addressed in turn.

A. Plaintiff Has Shown More Than a Speculative Fear That Her Telephone Metadata Has, Is, and Will Be Collected, and That Collection is a Search.

The Government states that "Plaintiff merely speculates…that metadata associated with her phone calls have been collected by the NSA." Dfs.' Opp. Br. at 12. The Government has not "declassified or *otherwise acknowledged* any further information regarding the identities of any other participating providers, past or present." Shea Decl. ¶ 17 (emphasis added).

Only the Government knows whether it is collecting Plaintiff's phone records. But, it is not acknowledging or denying it is doing so. Certainly, the Government is in the best position to tell the Court that is *not* collecting Plaintiff's phone records. The Plaintiff can not prove at this stage in the proceeding that it is not. However, despite the Government's lack of candor, the Court may reach the conclusion that the Government is collecting Plaintiff's phone records for the following reasons:

1. The Government declassified and authenticated the April 25, 2013 FISC Order signed by Judge Vinson and it confirms the Government collected phone records. *Klayman v. Obama*, 2013 WL 6571596 at * 15 (D.D.C. 2013).
2. The Government needs a complete database of all phone records to combat terrorism. *Id.*
3. A complete database is not possible without phone records of subscribers on the largest cell phone provider in the U.S. *Id.*
4. If the Government is not collecting phone records of nearly all Americans, the NSA database does not help the Government achieve its goal. *Id.*
5. The Government states that its collection of phone records is "an important means by which the National Security Agency (NSA)…has gathered information about communications among known and unknown terrorist actors in order to thwart future terrorist attacks." Dfs.' Opp. Br. at 1.
6. President Obama has essentially stated that the phone records of nearly all Americans are being collected and stored. Ex. G, Gilligan Decl.

Based on these facts, the Court can reasonably conclude for purposes of granting a preliminary injunction that Plaintiff's phone records are collected.

The Government cites to *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013), where the Supreme Court held that the plaintiffs lacked standing to challenge NSA surveillance under FISA because they only had a "highly speculative fear" that they were being targeted for surveillance. *Id* at 1147-50. This "speculative fear" was based upon a "speculative chain of possibilities." *Id.* This "chain of possibilities" did not demonstrate a "certainly impending" injury. *Id.*

Amnesty Int'l is distinguishable from the case at hand because of the Government's acknowledgements. Here, Plaintiff does not have a "highly speculative fear" that her metadata is being collected. According to the Government's own briefing, it has a "comprehensive metadata database" that allows it is determine who called who from up to three (now two) hops from "seed" number. See *Klayman*, 2013 WL 6571596 at *15. Applying *Amnesty Int'l*, it is clear that Plaintiff's fear is not "highly speculative." The fear is concrete. It is based upon a chain of possibilities that are real and for all intents and purposes admitted by the Government. The Plaintiff has standing to challenge the collection of her phone records.

B. Every Query of the Metadata Database is a Search.

The Government argues that "absent evidence that the 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." Dfs.' Opp. Br. at 15. At this stage in the proceeding, Plaintiff can not prove that her metadata has been "reviewed" by the NSA. Only the Government can say with certainty if it has and it does not.

This said, prior to January 17, 2014, the query process included a query of a "seed" number that resulted in call results from "three hops."[2] *Klayman*, 2013 WL 6571596 at *16. "When the NSA runs such a query, its system must necessarily analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number." *Id.* A query is a search of Plaintiff's call records. The Plaintiff has standing to challenge this search.

[2] Only "two hops" are now allowed. Ex. G, Gilligan Aff.

2. PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION SHOULD BE GRANTED.

The Government is correct that a preliminary injunction is an "extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7, 22, 129 S. Ct. 365, 172 L.Ed.2d 249 (2008). "To make this showing, the moving party must establish: (1) a likelihood of success on the merits; (2) a likelihood of irreparable harm to the moving party in the absence of preliminary relief; (3) that the balance of equities tips in favor of the moving party; and (4) that an injunction is in the public interest." *Battelle Energy Alliance, LLC v. Southfork Security, Inc.*, --- F. Supp. 2d. ---, 2013 WL 5818559 at *2 (D. Idaho Oct. 29, 2013) (citing *Winter*). "The requirements are stated in the conjunctive so that all four elements must be established to justify injunctive relief." *Id.* "The court may apply a sliding scale test, under which 'the elements of the preliminary injunction test are balanced, so that a stronger showing of one element may offset a weaker showing of another.'" *Id.* (citing *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011)).

However, the Court should be mindful that the Plaintiff is not seeking to enjoin an ordinary act, she is seeking to enjoin violation of her constitutional rights. "It has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

C. The Plaintiff Is Likely to Prevail in Proving that She Has a Reasonable Expectation of Privacy Interest in the Telephony Metadata She Creates.

The Plaintiff and the Government agree that *Smith v. Maryland* is the seminal case. *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577, 61 L.Ed.2d 220 (1979). But, disagree as to its

applicability in the 21st Century. In *Smith*, the Supreme Court held 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. 442 U.S. at 742, 99 S. Ct. 2577. The Plaintiff argues that *Smith* is distinguishable for the following reasons.

First, in *Smith*, the target of the surveillance was suspected of a crime. Plaintiff is not. Second, *Smith* only involved numbers dialed. Here, the Government is collecting call records on calls made, received, when the calls were made, the duration of the calls, and possibly where the phone was located at the time of the call. Third, the scope of the program includes millions of Americans and only was person was targeted in *Smith.*

In response, the Government attempts to explain away each these arguments. First, the Government argues that whether a person is under an individualized suspicion of a crime does not matter. Dfs.' Opp. Br. at 20. The Government states "[t]his 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." *Id.* In short, the collection of phone records is not a "search". Therefore, the Fourth Amendment is inapplicable. However, the Government does not explain why it was a "search" in *Smith* to collect phone records of a criminal suspect, but it is not a "search" here. There is no difference. Such a collection call records was a "search" in *Smith*, and it is a "search" here.

The Government also disputes that *Smith* is distinguishable because it only involved the collection of *numbers dialed*. Here, the Government is collecting not only who the Plaintiff calls, but also who calls the Plaintiff, when the calls occur, and how long the calls last. To downplay this difference, the Government argues that "[j]ust 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." Dfs.' Opp. Br. at 20. However, the scope of the search certainly goes to its reasonableness and distinguishes *Smith* from this case.

The Government cites to a Ninth Circuit Court of Appeals case, *United States. v. Reed*, 575 F.3d 900 (9th Cir. 2009), for the proposition that 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'". Dfs.' Opp. Br. at 20 (citing to *U.S. v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009)). *Reed* is distinguished by the fact that the Government received a federal wiretap order. *Reed*, 575 F.3d at 905.[3] In addressing whether the wiretap evidence should be suppressed, because the Government failed to seal call data from the tapped line, the Court of Appeals held that the call data "is not an intercepted communication falling within the sealing requirements of [18 U.S.C.] § 2518(8)." *Id.* at 914. The call data collected was "call origination, length, and time of call." *Id.* In other words, the call data collected encompassed the information collected by the pen register and/or trap and trace device. *Id.* Because call data collected was "nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy'" under *Smith*. *Id.* (citing *Smith v. Maryland*, 442 U.S. 735, 743–44, 99 S. Ct. 2577, 61 L.Ed.2d 220 (1979)). This statement is dicta. *Reed* is helpful because it supports the conclusion that the

[3] In *Reed*, Reed moved to suppress the evidence gathered under the wiretap order. *Id*. at 907. The District Court denied Reed's motion to suppress. *Id.* Reed was convicted and sentenced to life in prison. *Id.* Reed appealed. *Id*. at 908. Reed argued that the district court erred in denying the motion to suppress wiretap evidence, because (1) the Government failed to show necessity for the wiretap, as required by 18 U.S.C. §§ 2518(1)(c) & (3)(c); (2) the wiretap was not discontinued after the Government learned that phone tapped was primarily used by another person; (3) the Government colluded with the telephone company to make illegally intercepted calls appear as though they were lawfully intercepted; (4) the Government failed to timely seal the recordings, and completely failed to seal transcripts from calls on the phone line; and (5) the wiretap was not properly monitored by federal agents. *Id.* After examining the various wire tapping statutes, the Court ultimately concluded that the call data collected was "not an intercepted communication of any sort and does not contain the content of an intercepted wire, oral or electronic communication, we hold that it is not subject to the recordation and sealing requirements of § 2518(8)." Id. at 917.

collection of phone records is a "search". However, it does not address whether such a search is reasonable outside of a criminal investigation.

Third, the Government argues that the fact it is collecting telephony metadata on millions of Americans is irrelevant. Dfs.' Opp. Br. at 20. Plaintiff concedes that Fourth Amendment rights "are personal in nature." *Steagald v. United States*, 451 U.S. 204, 219 (1981). However, the scope of the Government's dragnet distinguishes *Smith* – where there was only one pen register targeting one person. Here, the Plaintiff's *and* millions of American's Fourth Amendment rights are being violated on a daily basis for years. In an attempt to divert the Court's attention from this fact, the Government states that 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." Dfs.' Opp. Br. at 21-22. Plaintiff disagrees. Here, the Plaintiff's phone records are being collected on a daily basis and stored for five years. The collection has been going on for seven years. It will likely continue as long as the U.S. is battling a terrorism threat. These phone records "reflect a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). Contrast this with *Smith*, where the collection occurred between March 6, 1976 and March 19, 1976, and there is no indication from the Court's opinion that it expected the Government to retain those limited phone records once the case was over. *See Smith*, 442 U.S. at 737, 99 S. Ct. 2577. In *Jones*, the GPS tracking device was in place for four weeks. *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring). It was found to violate the reasonable expectation of privacy. *Id*. The argument that the targeted, highly-limited data

collection about a criminal is less invasive than the daily, perpetual collection of Plaintiff's private information that is stored for years is specious.

As to the Government's argument that the Plaintiff can not show her information was ever reviewed by an NSA analyst, at this stage in the proceeding, the statement is true. In fact, it may be true that a real person has never reviewed the Plaintiff's call logs. However, every query of a "seed" number requires Plaintiff's call logs to be searched. This is a search. Moreover, the Government has the ability to store "such records and efficiently mine them for information years into the future." *Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring). This a real threat of a violation of Plaintiff's Fourth Amendment rights.

The Government also argues that if the information was reviewed, the Government does not know who any of the telephone numbers belong to. Dfs.' Opp. Br. at 22. However, in order to get that information the FBI must issue a national security letter ("NSL") to the phone company. NSLs do not require *any* judicial oversight, *see* 18 U.S.C. § 2709; 12 U.S.C. § 3414, 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 3162, meaning they are hardly a check on potential abuses. There is also nothing stopping the Government from skipping the NSL step altogether and using public databases or any of its other vast resources to match phone numbers with subscribers. *See, e.g.,* James Ball et al., *Covert surveillance: The reaction: 'They are tracking the calling patterns of the entire country',* GUARDIAN, June 7, 2013, at 5 ("[W]hen cross-checked against other public records, the metadata can reveal someone's name, address, driver's licence, credit history, social security number and more."). It appears the Government would simply have the Plaintiff trust that it will not abuse its power.

Finally, the Government argues that the metadata in *Smith* is the same as the phone records collected today. Dfs.' Opp. Br. at 24. But, the phone records collected today are

different. Today, the phone records reveal whether calls were connected and how long the conversation lasted. *See Klayman*, 2013 WL 6571596 at *21, fn. 57. Moreover, the trunk identifier is collected. Dfs.' Opp. Br. at 6. This can be used to track a caller's location, which was not possible in 1979.[4] *Klayman*, 2013 WL 6571596 at *21, fn. 57. *Klayman*, 2013 WL 6571596 at *21.

Thus, the question the Court must answer is whether society is prepared to recognize as objectively reasonable and justifiable the Plaintiff's expectation of privacy in her phone records. Phone records that create a detailed picture of familial, political, professional, and religious associations. The Court does not have to answer the question today. However, if it finds that Plaintiff is likely to prevail, it should grant Plaintiff's motion for a preliminary injunction and deny the Governments motion to dismiss.

D. There is a High Likelihood of Irreparable Harm to Plaintiff in the Absence of Preliminary Relief.

The Government argues that the Plaintiff is not "suffering any consequences as a result of the telephony metadata program, much less injury so grave as to constitute irreparable harm." Dfs.' Opp. Br. at 28. The Government apparently ignores that "[i]t has long been established that the loss of constitutional freedoms, 'for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

---

[4] "A trunk identifier 'can reveal where [each] call enter[s] the trunk system' and can be used to 'locate a phone within approximately a square kilometer,' Patrick Di Justo, *What the N.S.A. Wants to Know About Your Calls*, NEW YORKER (June 7, 2013), http:// www.newyorker.com/online/blogs/elements/2013/06/what-the-nsa-wants-to-know-about-your-phone-calls.html. And 'if [the metadata] includes a request for every trunk identifier used throughout the interaction,' that "could allow a phone's movements to be tracked.' *Id.* Recent news reports, though not confirmed by the Government, cause me to wonder whether the Government's briefs are entirely forthcoming about the full scope of the Bulk Telephony Metadata Program. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA maps targets by their phones*, WASH. POST, (Dec. 5, 2013), at A01." *Klayman*, 2013 WL 6571596 at *21, fn. 57.

E. The Balance of the Equities Favor Plaintiff.

In response to the argument that the equities favor the Plaintiff, the Government states that it "would be extremely burdensome" for the NSA to comply with a preliminary injunction. Dfs.' Opp. Br. at 28. In short, it is too hard to abide by the Fourth Amendment. The Government does not cite to any case that has held there is an exception to following the Fourth Amendment because it is "extremely burdensome" to do so. The balance of the equities tip in Plaintiff's favor.

F. An Injunction is in the Public Interest.

Plaintiff agrees with the Government that the public interest in preventing terrorist attacks is great. But, so is the interest in protecting the Constitutional rights of Americans. As the 2nd Circuit Court of Appeals noted and the Government does not dispute: "It is always in the public interest to prevent the violation of a party's constitutional rights." *Melendres v. Arpaio*, 695 F.3d 990, 1002 (9th Cir. 2012). Thus, the public interest in protecting rights under the Fourth Amendment weighs heavily in favor of Plaintiff. The motion for preliminary relief must be granted and the Government's motion to dismiss denied.

PLAINTIFF'S STATUTORY AND FIRST AMENDMENT CLAIMS

Upon careful review of the Government's argument and the supporting authority, Plaintiff concedes that her claims that the collection of her phone records violates statutory law and the First Amendment may be dismissed.

CONCLUSION

The case is an example of the difficult balance between the Government's interest in protecting the homeland and an individual's freedom from search by the Government. In this case, Plaintiff urges the Court to find for the side of freedom and grant her motion for a

preliminary injunction and enter an order that (1) bars the Government from collecting any telephony metadata associated with her Verizon Wireless account and (2) require the Government to destroy any such metadata in its possession. The Plaintiff also asks the Court to deny the Government's Motion to dismiss her claims under the Fourth Amendment.

DATED this 21st day of February, 2014.

LUKINS & ANNIS, P.S.

By /s/ *Peter J. Smith IV*
PETER J. SMITH IV, ISB 6997
Co-Counsel for Plaintiff
ANNA J. SMITH