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,

VS.

Plaintiff,

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

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION

Table of Contents

TABLE OF AUTHORITIES	3
INTRODUCTION	4
REVELATION THAT NSA WAS COLLECTION PHONE RECORDS OF MILLIONS OF AMERICANS	4
STATUTORY BACKGROUND	5
1. FISA and Section 215 of the Patriot Act (50 U.S.C. § 1861 (2013))	5
2. The Government's Collection of Telephony Metadata Program	7
3. Collection of Smith's Call Records	7
ARGUMENT	7
1. This Court has jurisdiction over the Constitutional challenges to the Government's conduct	7
2. Smith has standing to challenge the collection of bulk telephony metadata and analysis by the government	
3. Preliminary Injunction	11
a) Smith is likely to succeed on the merits	11
b) Smith will suffer irreparable harm in the absence of preliminary relief	15
c) The balance of equities tips in Smith's favor	15
d) An injunction is in the public interest.	15
CONCLUSION	16

TABLE OF AUTHORITIES

CASES

Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013)	5, 8, 9, 11
Elrod v. Burns, 427 U.S. 347, 373 (1976)	
Ferguson v. Charleston, 532 U.S. 67 (2001)	14
Klayman v. Obama, Case 1:13-cv-00851 (RJL) (S.D.N.Y. 2013)	
Kyllo v. United States, 533 U.S. 27, 33 (2001)	12
Melendres v. Arpaio, 695 F.3d 990, 1002 (9th Cir. 2012)	16
Smith v. Maryland, 442 U.S. 735 (1979)	
Stormans, Inc. v. Selecky, 586 F.3d 1109, 1127 (9th Cir. 2009)	11
United States v. Jones, 132 S. Ct. 945 (2012)	12, 13, 14, 15
Webster v. Doe, 486 U.S. 592 (1988)	8
Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 20 (2008)	11
STATUTES	
50 U.S.C. § 1803 (2013)	5
50 U.S.C. § 1861 (2013)	5, 6
OTHER AUTHORITIES	
Administration White Paper: Bulk Collection of Telephony Metadata under Section 2015 of the ACT (August 9, 2013)	USA PATRIOT 10, 11, 12, 13
Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, GUARDI 5, 2013	AN (London), June
Grading the top U.S. carriers in the third quarter of 2013, FIERCEWIRELESS.COM (Nov. 18, 2013	5) 9
Primary Order, In re Application of the [FBI] for an Order Requiring the Production of Tangible [Redacted], No. BR 13-158	7
Secondary Order, In re Application of the [FBI] for an Order Requiring the Production of Tangia Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/o Services, No. BR 13-80	a Verizon Business
RULES	
FISC Rule of Procedure 17	5
CONSTITUTIONAL PROVISIONS	
U.S. CONST. amend IV	
U.S. CONST. art. III. § 2	7

INTRODUCTION

For the last seven years, the National Security Agency ("NSA") has kept a record of every call made by the Plaintiff, Anna Smith ("Smith"). The records show who Smith called; when Smith called; and how long Smith talked. With this information, the government has a detailed picture of who Smith interacts with, and when Smith interacts with them.

On June 12, 2013, Smith filed a lawsuit to stop the collection of her phone data and purge the database of any existing records. Smith contends that the ongoing tracking of her phone calls exceeds the statutory authority and violates the First and Fourth Amendment. Smith asks this Court to, *inter alia*, to permanently enjoin the government from collecting her phone records and purge the database of her records. During the pendency of this action, Smith moves for a preliminary injunction that (i) bars the collection of metadata from her calls; (ii) requires the government to locate and separate Smith's metadata records; and (iii) bars the government from querying the metadata information it already possesses.

If this preliminary injunction is not granted, Smith will suffer irreparable injury because her constitutional rights will be violated on a daily basis. Smith's metadata records will continue to be collected and queried. As explained below, preliminary relief is appropriate and undeniably necessary.

REVELATION THAT NSA WAS COLLECTING PHONE RECORDS OF MILLIONS OF AMERICANS

This case arose from a revelation by Edward Snowden. On June 5, 2013, *The Guardian* newspaper reported that the government was engaging in dragnet surveillance of U.S. citizens. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*,

GUARDIAN (London), June 5, 2013. According to the Foreign Intelligence Surveillance Court order provided to the GUARDIAN by Edward Snowden, Verizon Business Networks Services ("VBNS") was required to produce to the NSA on "an ongoing daily basis...all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services*, No. BR 13-80 at 2 (FISC April. 25, 2013) ("April 25, 2013 Secondary Order") (attached as Ex. 1 to P. Smith Decl. filed herewith).²

STATUTORY BACKGROUND

1. FISA and Section 215 of the Patriot Act (50 U.S.C. § 1861 (2013))

In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to "authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013). FISA created the Foreign Intelligence Surveillance Court ("FISC"). *See* 50 U.S.C. § 1803(a) (2013). The FISC is empowered to issue surveillance orders in foreign-intelligence investigations in secret. *Id.*; *see*, *e.g.*, FISC Rule of Procedure 17(b).³

The provision of the law at issue in this case is commonly referred to as Section 215. 50 U.S.C. § 1861. It allows the government to obtain an order from the FISC requiring the production of "any tangible things (including books, records, papers, documents, and other

1

¹ Available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

² The government admitted the authenticity of the order although aspects of the program remain classified, including whether Verizon Wireless is compelled to provide metadata information to the NSA. The government has released information about the program. *See* Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA PATRIOT ACT (August 9, 2013), *available at* http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/.

³ http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

items)" if the government shows that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)...to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2)(A).

There are certain "safeguards" to the use of such information. For example, any investigation must be authorized and conducted under the guidelines approved by the Attorney General under Executive Order No. 12,333 (or a successor thereto). 50 U.S.C. § 1861(a)(2)(A), (b)(2)(A). An application for such an order must "enumerat[e]...minimization procedures adopted by the Attorney General...that are applicable to the retention and dissemination by the [FBI] based on the order requested." 50 U.S.C. § 1861(b)(2)(A). "Minimization procedures" are "specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting [U.S.] persons consistent with the need of the [U.S.] to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1861(g)(2). Upon finding that such a burden has been met, the FISC "shall enter an ex parte order as requested, or as modified, approving the release of tangible things." 50 U.S.C. § 1861(c)(1). The ex parte order is referred to as a "production order." 50 U.S.C. § 1861(f)(1)(A).

The information gathered pursuant to a production order "concerning any [U.S.] person may be used and disclosed by Federal officers and employees without the consent of the [U.S.] person only in accordance with the minimization procedures adopted" by the Attorney General and approved by the FISC. 50 U.S.C. § 1861(h). However, the recipients of a production order may not disclose its existence to anyone. 50 U.S.C. § 1861(d)(1).

2. The Government's Collection of Telephony Metadata Program

The government has collected bulk telephony metadata for more than seven years.

Klayman v. Obama, Case 1:13-cv-00851 (RJL) (S.D.N.Y. 2013) filed December 16, 2013 at pg.

16. In Klayman v. Obama, Case 1:13-cv-00851 (RJL) District Judge Richard J. Leon, in a written decision filed December 16, 2013, described in detail how the program operates. This description was based almost entirely upon the government's own affidavits and briefing. Klayman v.

Obama, Case 1:13-cv-00851 (RJL) filed December 16, 2013 at pg. 16-23. This detail will not be repeated in this memorandum, but is incorporated herein.

3. Collection of Smith's Call Records

Smith is a Verizon Wireless customer. A. Smith Decl. filed herewith at ¶ 2. As a current customer of Verizon Wireless, Smith has had her telephony metadata collected in bulk pursuant to the April 25, 2013 Secondary Order, its predecessors and, now, its successors. This collection of telephony metadata continues on "an ongoing daily basis." April 25, 2013 Secondary Order at 2. The most recent FISC production order expires on January 3, 2014. Primary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-158 (attached as Ex. 3 to P. Smith Decl. filed herewith).

ARGUMENT

1. This Court has jurisdiction over the Constitutional challenges to the Government's conduct.

Smith raises a challenge to the government's conduct under the First and Fourth Amendments of the United States Constitution. Whether a Constitutional violation exists, is decided by this Court under the authority granted to it under Article III of the United States Constitution. U.S. CONST. art. III, § 2. The only possible argument against this Court's

jurisdiction that could be raised is whether Congress precluded judicial review by non-FISC courts of the Constitutional claims related to production orders issued by FISC courts. Such an argument fails.

In Webster v. Doe, 486 U.S. 592 (1988), the United States Supreme Court stated that "where Congress intends to preclude judicial review of constitutional claims its intent to do so must be clear." *Id.* at 603. This is required 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." *Id.* In other words, a statute may be challenged unless Congress clearly states otherwise.

FISA does not expressly preclude judicial review of constitutional claims. Admittedly, it does not expressly allow them either. However, the presumption that federal district courts may hear a constitutional claim is clear and, so, any preclusion of constitutional claims must also be clearly stated in the statute. *Webster*, 486 U.S. at 603. Here, FISA contains no such preclusion. The Court has jurisdiction to hear Smith's constitutional claim.

2. Smith has standing to challenge the collection of bulk telephony metadata and analysis by the government

"To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 (2013) (internal quotation marks omitted). In *Clapper*, 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*.

This case is different. The bulk collection of telephony metadata involves two Fourth Amendment searches: (1) collection of metadata and (2) analysis of metadata. Smith may challenge both searches. First, Smith does not *speculate* about whether metadata from her calls is collected; the government has essentially conceded it is taking place. Here, the government has declassified and authenticated an April 25, 2013 Secondary Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony metadata from VBNS as part of a broad program. April 25, 2013 Secondary Order.

The government will likely argue that the April 25, 2013 Secondary Order only applies to VBNS – not Verizon Wireless. Therefore, there is no proof that metadata of Smith has been collected, retained and queried without any reasonable suspicion. However, the government surveillance will only be effective if it has a comprehensive metadata database. Verizon Wireless is the single largest wireless carrier in the United States. *See Grading the top U.S. carriers in the third quarter of 2013*, FIERCEWIRELESS.COM (Nov. 18, 2013). In its own white paper, the government explained that collecting metadata from all domestic cell phones was imperative to the potency of the program:

International terrorist organizations and their agents use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. In addition, when they are located inside the United States, terrorist operatives make domestic U.S. telephone calls. The most analytically significant terrorist-related communications are those with one end in the United States or those that are purely domestic, because those communications are particularly likely to identify suspects in the United States—whose activities may include planning attacks against the home land. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are communicating with others inside the United States, as well as communications

-

⁴ http://www.fiercewireless.com/special-reports/grading-top-us-carriers-third-quarter-2013.

between operatives within the United States. <u>In this respect, the program helps to close critical intelligence gaps that were highlighted by the September 11, 2001 attacks.</u>

. . .

The national security objectives advanced by the telephony metadata program would therefore be frustrated if the NSA were limited to collection of a narrower set of records. In particular, a more restrictive collection of telephony metadata would impede the ability to identify a chain of contacts between telephone numbers, including numbers served by different telecommunications service providers, significantly curtailing the usefulness of the tool. This is therefore not a case in which a broad collection of records provides only a marginal increase in the amount of useful information generated by the program. Losing the ability to conduct focused queries on bulk metadata would significantly diminish the effectiveness of NSA's investigative tools.

..

Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls.

Administration White Paper: Bulk Collection of Telephony Metadata under Section 2015 of the USA PATRIOT ACT (August 9, 2013) (emphasis added).⁵ If the largest domestic wireless carrier is not part of the program, then there is a "critical intelligence gap" in the program. As Judge Leon stated, the implausibility that Verizon Wireless customers' metadata is not collected "defies common sense and does not exactly inspire confidence!" *Klayman v. Obama*, Case 1:13-cv-00851 (RJL) filed December 16, 2013 at pg. 38.

Not only does a search occur when the data is collected, it is also searched each time the government queries the database. Each time a search occurs, the government <u>must</u> search everyone's metadata. As explained in the government's own white paper, when a "seed" number is queried, it is imperative that the entire database be searched to see if any other person called or received a call from that "seed".

Thus, critically, although a large amount of metadata is consolidated and preserved by the Government, the vast majority of that information is never seen by any person. Only

⁵ http://apps.washingtonpost.com/g/page/politics/obama-administration-white-paper-on-nsa-surveillance-oversight/388/

information responsive to the limited queries that are authorized for counterterrorism purposes is extracted and reviewed by analysts. Although the number of unique identifiers has varied substantially over the years, in 2012, fewer than 300 met the "reasonable, articulable suspicion" standard and were used as seeds to query the data after meeting the standard. Because the same seed identifier can be queried more than once over time, can generate multiple responsive records, and can be used to obtain contact numbers up to three "hops" from the seed identifier, the number of metadata records responsive to such queries is substantially larger than 300, but it is still a tiny fraction of the total volume of metadata records. It would be impossible to conduct these queries effectively without a large pool of telephony metadata to search, as there is no way to know in advance which numbers will be responsive to the authorized queries.

Administration White Paper: Bulk Collection of Telephony Metadata under Section 2015 of the USA PATRIOT ACT (August 9, 2013). When one considers that this information is updated daily, new information about almost every American is collected and searched every day.

Smith meets the standing requirement set forth in *Clapper*. Smith clearly demonstrated it is extremely probable that the NSA has collected and analyzed telephony metadata on almost every American. The injury to Smith is concrete, particularized, actual and imminent. It is fairly traceable to the challenged action and redressable by a favorable ruling by this Court.

3. **Preliminary Injunction**

The proper legal standard for preliminary injunctive relief requires a party to demonstrate:

- 1. That she is likely to succeed on the merits;
- 2. That she is likely to suffer irreparable harm in the absence of preliminary relief;
- 3. That the balance of equities tips in her favor; and
- 4. That an injunction is in the public interest.

Stormans, Inc. v. Selecky, 586 F.3d 1109, 1127 (9th Cir. 2009), quoting Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 20 (2008). Each of these elements will be addressed below.

a) Smith is likely to succeed on the merits.

Smith has shown that she is likely to succeed on her Fourth Amendment claims. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend IV. That right "shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.* When "the Government obtains information by physically intruding on a constitutionally protected area" a search occurs. *United States v. Jones*, 132 S. Ct. 945, 950 n.3 (2012). A search also occurs when "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Clearly, the latter search applies in this case. The fundamental question is: Does Smith have a subjective expectation of privacy that society recognizes as reasonable?

To answer this question, the Court must compare this case to *Smith v. Maryland*, 442 U.S. 735 (1979). The government relies on *Smith* as authority for its collection of metadata about almost every American. Administration White Paper: Bulk Collection of Telephony Metadata under Section 2015 of the USA PATRIOT ACT (August 9, 2013). The Government states:

A Section 215 order for the production of telephony metadata is not a "search" as to any individual because, as the Supreme Court has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that the Government's collection of dialed telephone numbers from a telephone company did not constitute a search of the petitioner under the Fourth Amendment, because persons making phone calls lack a reasonable expectation of privacy in the numbers they call. *Id.* at 743-46. Even if a subscriber subjectively intends to keep the numbers dialed secret, the Court held, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. The Court explained that someone who uses a phone has "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," and therefore has "assumed the risk that the company would reveal to the police the numbers [] dialed." *Id.* at 744.

Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing,

addressing, or signaling information, under the reasoning adopted by the Supreme Court in *Smith* there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes. Under longstanding Supreme Court precedent, this conclusion holds even if there is an understanding that the third party will treat the information as confidential.

Id.

Smith is distinguishable in several key aspects. First, *Smith* involved the installation of a pen register on Smith's phone because he was believed to have made threatening and obscene phone calls to a robbery victim. *Smith*, 442 U.S. at 737. When Smith dialed a phone number, the government knew what number was dialed. *Id.* The Supreme Court held that Smith had no reasonable expectation of privacy in the numbers he dialed from his phone because he voluntarily transmitted them to his phone company, and because it is generally known that phone companies keep such information in their business records. *Id.* at 742-44.

Here, however, the government is using its surveillance power to gather information on almost every American before even a suspicion of a crime exists. The fact that the government can demand and receive a data dump of telephony metadata, which includes information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted, is completely different than a pen register that only tracked what numbers were called.

The Supreme Court recognized that it may be time to revisit how *Smith* is applied in the digital age. In *United States v. Jones*, 132 S. Ct. 945 (2012), five justices found that law enforcement's use of a GPS device to track a vehicle's movements for nearly a month violated Jones's reasonable expectation of privacy. *Id.* at 955-56. The GPS device in *Jones* was only in place for a month, but the Supreme Court still stated that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 964 (Alito, J.,

concurring). Admittedly, under the production orders that have been disclosed, the government is not using telephony metadata to track the movements of Americans. However, the same kind of long term surveillance is taking place. The government is gathering data that shows who Smith calls, when she calls them, how long she talks to them, and the number she reaches them at. This information, when gathered in aggregate over 5 years, can reveal a great deal of private information about a person. *See* Declaration of Professor Edward W. Felten filed in the United States District Court Southern District of New York on August 26, 2013 in *American Civil Liberties Union et al. v. Clapper*, Case 1:13-cv-03994-WHP attached as Exhibit "5" to P. Smith Decl. filed herewith. By contrast, in *Smith*, the pen register was only operational between March 6 and March 19, 1976. *Smith*, 442 U.S. at 737. In *Jones*, the tracking was in place for a month and it was unconstitutional. Here, Smith's calling history is 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. *See Klayman*.

Also in stark contrast to this case, in *Smith*, the pen register was installed at the central office of the phone company. *Smith*, 442 U.S. at 737. Here, the government and the wireless carriers of America have entered into a formalized arrangement where the wireless carriers collect the information and turn it over to the government. The government is not collecting the metadata, it is having it delivered (i.e., data dumped) every day into its system. When the government does not actually collect the information, it raises serious Fourth Amendment concerns. *See Ferguson v. Charleston*, 532 U.S. 67 (2001).

Finally, *Smith* is distinguishable because the scope of the search was one person. Here, the government is collecting telephony metadata of *hundreds of millions of people every single day*. The scope of the program today is clearly a fact that distinguishes *Smith*. One does not need

an expert to opine that the use of cell phones have grown more each year. All one needs to do is walk down the street. The huge growth in cell phone use means that the the government collects, retains and queries metadata that "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring). This is certainly true of Smith who uses her cell phone 99% of the time to make calls. Smith Decl. filed herewith at 3.

The actions challenged here are clearly distinguishable from those in *Smith*. The collection of metadata on every one of Smith's cell phone calls every day and storage of that information for five years certainly violates her subjective expectation of privacy and, when the Court hears this case in its entirety, it will surely find that she has a reasonable expectation of privacy in the metadata that is created by her everyday use of her cell phone. As such, this Court should find that she is likely to succeed in this case.

b) Smith will suffer irreparable harm in the absence of preliminary relief.

"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) (plurality opinion). As stated above, Smith is suffering from an unreasonable search that violates the Fourth Amendment. Such a violation of her constitutional rights is an irreparable injury.

c) The balance of equities tips in Smith's favor.

As explained above, Smith has established that the gather of all telephony metadata she creates is an unreasonable search. When faced with this type of intrusive governmental activity, the balance of equities clearly tips in her favor.

d) An injunction is in the public interest.

Case 2:13-cv-00257-BLW Document 8-1 Filed 12/20/13 Page 16 of 17

"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). Therefore, it is clearly within

the discretion of this Court to grant preliminary injunctive relief when a party's constitutional

rights are violated. The government will likely argue that the removal of metadata collected

about Smith will throw the entire program into danger. However, her removal will not degrade

the program. The risk of Smith's call chains destroying the effectiveness of the program is not a

risk.

CONCLUSION

The case is a perfect 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, Smith 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.

DATED this 20th day of December, 2013.

LUKINS & ANNIS, P.S.

 $\mathbf{R}\mathbf{v}$

PETER J. SMITH IV, ISB 6997

Co-Counsel for Plaintiff

ANNA J. SMITH

CERTIFICATE OF SERVICE

I hereby certify that on this 20th day of December, 2013, I served a true and correct copy of the foregoing MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION by the method described below to:

JAMES J. GILLIGAN Special Litigation Counsel U.S Department of Justice Civil Division, Federal Programs Branch 20 Massachusetts Ave., N.W., Room 6102 Washington, D.C. 20001		U.S. Mail Hand Delivered Overnight Mail Telecopy (FAX) (202) 616-8470 Electronic Mail james.gilligan@usdoj.gov
MARCIA BERMAN Senior Trial Counsel U.S Department of Justice Civil Division, Federal Programs Branch 20 Massachusetts Ave., N.W., Room 7132 Washington, D.C. 20001		U.S. Mail Hand Delivered Overnight Mail Telecopy (FAX) (202) 616-8470 Electronic Mail marcia.berman@usdoj.gov
RODNEY PATTON Trial Attorney U.S Department of Justice Civil Division, Federal Programs Branch 20 Massachusetts Ave., N.W., Room 7320 Washington, D.C. 20001		U.S. Mail Hand Delivered Overnight Mail Telecopy (FAX) (202) 616-8470 Electronic Mail rodney.patton@usdoj.gov
SYRENA C. HARGROVE Assistant United States Attorney District of Idaho Washington Group Plaza Iv 800 E. Park Boulevard, Suite 600 Boise, ID 83712-9903		U.S. Mail Hand Delivered Overnight Mail Telecopy (FAX) (208) 334-1414 Electronic Mail Syrena.Hargrove@usdoj.gov
	P	IS &