No. 14-35555

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ANNA J. SMITH,

Plaintiff - Appellant,

v.

BARACK OBAMA, *et al*.,

Defendants - Appellees.

On Appeal from the United States District Court
for the District of Idaho, Boise; Case No. 2:13-cv-00257-BLW
The Honorable B. Lynn Winmill, Chief District Judge

APPELLANT'S EXCERPTS OF RECORD VOLUME II

Peter J. Smith IV
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
LUKE MALEK, ATTORNEY
AT LAW, PLLC
721 N 8th Street
Coeur d'Alene, ID 83814
Phone: 208-661-3881
Email:
Luke_Malek@hotmail.com

Cindy Cohn
David Greene
Hanni Fakhoury
Andrew Crocker
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: cindy@eff.org

Jameel Jaffer
Alex Abdo
Patrick Toomey
AMERICAN CIVIL
LIBERTIES UNION
FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 549 2500
Facsimile: (212) 549-2654
Email: jjaffer@aclu.org

Richard Alan Eppink
AMERICAN CIVIL
LIBERTIES UNION OF
IDAHO FOUNDATION
P.O. Box 1897
Boise, ID 83701
Telephone: (208) 344-9750
Facsimile: (208) 344-7201
Email: reppink@acluidaho.org

Counsel for Plaintiff-Appellant Anna J. Smith

INDEX VOLUME ONE

INDEX VOLUME TWO

DATED: September 2, 2014 Respectfully submitted,

By: */s/ Peter Smith*
Peter J. Smith IV

LUKINS & ANNIS, P.S.
601 E. Front Avenue, Suite 502
Coeur d'Alene, ID 83814

Lucas T. Malek
LUKE MALEK, ATTORNEY AT LAW, PLLC
721 N 8th Street
Coeur d'Alene, ID 83814

Cindy Cohn
David Greene
Hanni Fakhoury
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jameel Jaffer
Alex Abdo
Patrick Toomey
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004

Richard Alan Eppink
AMERICAN CIVIL LIBERTIES UNION OF IDAHO FOUNDATION
P.O. Box 1897
Boise, ID 83701

Counsel for Plaintiff-Appellant ANNA J. SMITH

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on September 2, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: September 2, 2014

Respectfully submitted,

By: *__/s/ Peter Smith____*
Peter J. Smith IV
LUKINS & ANNIS, P.S.

Counsel for Plaintiff-Appellant ANNA J. SMITH

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-BLW **PLAINTIFF'S NOTICE OF APPEAL**

NOTICE IS HEREBY GIVEN that Plaintiff Anna J. Smith hereby appeals to the United States Court of Appeals for the Ninth Circuit from the Judgment entered in this action on June 3, 2014 [Docket #28], granting Defendants' motion to dismiss Plaintiff's complaint and denying Plaintiff's motion for a preliminary injunction.

DATED this 1st day of July, 2014.

LUKINS & ANNIS, P.S.

By _____
PETER J. SMITH IV, ISB 6997
Co-Counsel for Plaintiff
ANNA J. SMITH

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.	Case No. 2:13-CV-257-BLW **JUDGMENT**

In accordance with the Memorandum Decision filed with this Judgment,

NOW THEREFORE IT IS HEREBY ORDERED, ADJUDGED, AND DECREED, that the motion for injunction (docket no. 8) is DENIED.

IT IS FURTHER ORDERED, ADJUDGED, AND DECREED, that the motion to dismiss (docket no. 14) is GRANTED, and the Clerk is directed to close this case.

DATED: June 3, 2014

B. Lynn Winmill
Chief Judge
United States District Court

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

--oOo--

CERTIFIED COPY

ANNA JO SMITH,
Plaintiff,

vs.

BARACK H. OBAMA, et al.,
Defendant.

No. 2:13-cv-257-BLW

REPORTER'S TRANSCRIPT OF AUDIOTAPED PROCEEDINGS

May 15, 2014

APPEARANCES:

For the Plaintiff:

BY: PETER J. SMITH, IV
LUKINS & ANNIS
601 E. Front Avenue, #502
Coeur d'Alene, Idaho 83814

For the Defendant:

BY: MARCIA BERMAN
US DEPARTMENT OF JUSTICE
CIVIL DIVISION, FEDERAL
PROGRAMS BRANCH
20 Massachusetts Ave., NW,
Room 7132
Washington, D.C. 20001

Transcribed by: VALERIE NUNEMACHER, CSR, CCR, RPR

1 PROCEEDINGS May 15, 2014
2 --oOo--
3 THE CLERK: United States District Court for
4 the District of Idaho is now in session. The Honorable
5 B. Lynn Winmill presiding.
6 THE COURT: Thank you. Please be seated.
7 THE CLERK: The Court will now hear civil case
8 13-CV-257-BLW. Smith versus Obama, et al.
9 THE COURT: Good morning, counsel. Give me
10 just a moment to get set up here.
11 All right. Counsel, I have reviewed the
12 briefing in this matter in some detail. It does seem to
13 me that given the Supreme Court's decision, albeit,
14 what, 30 years ago or 35 years ago, in the Smith case,
15 that that's the challenge in this case.
16 How is this case really distinguishable from
17 the Supreme Court's pronouncement? Now, the argument
18 has been made that just the passage of time and the
19 advent of new technology should be sufficient for the
20 Court as I think the -- as Judge Leon, I think, did in
21 the Klayman case, just say a different result is
22 necessary here.
23 But I am a real believer in -- in fact, I gave
24 a speech two days ago in Boise, on the rule of law and
25 talked at great length about the need for kind of

1 restraint on the part of the judiciary and not ignoring
2 several principles.
3 Now, that doesn't mean that there aren't
4 occasions where that has to happen, but the question is
5 why -- what has happened in the intervening 35 years
6 that would change our assessment or is that case simply
7 distinguishable?
8 I think, also, what corollaries can we draw
9 from the Jones' case more recently is also, I think,
10 perhaps an important issue. But I think that's really
11 what this case turns on. I know there's a lot of
12 argument about standing and other issues, but I think
13 the more critical issue is that issue of whether or not
14 there is an expectation of privacy here and I think the
15 case really is going to turn on that issue.
16 So with that, I'm not sure who's going to
17 argue for the plaintiffs --
18 MS. BERMAN: Not the plaintiffs.
19 THE COURT: Ms. Berman, is it?
20 MS. BERMAN: For the defense, defendants.
21 THE COURT: Well, no, I -- I'm sorry, we have
22 our tables, normally -- you all set up in the wrong
23 order. Sorry. The plaintiffs, that's what I should
24 have been, usually -- we're turned around.
25 MS. BERMAN: Sorry.

1 THE COURT: Mr. Smith, you're going to --
2 MR. SMITH: I'm going to argue on behalf of
3 the plaintiff, your Honor.
4 THE COURT: Very well, thank you. I guess
5 it's that the government is always sitting there.
6 That's what threw me off a little bit, so...
7 MR. SMITH: They're normally carrying the
8 burden, correct, your Honor?
9 THE COURT: True. In 90 percent of the cases
10 I have because they're all criminal matters.
11 Mr. Smith.
12 MR. SMITH: Your Honor, thank you very much.
13 My name is Peter Smith. I represent the plaintiff, Anna
14 Smith, who happens to be my lovely wife.
15 Co-counsel with me is Luke Malek from Coeur
16 d'Alene as well. And this is my first time being able
17 to argue before your Honor and I'm honored to have the
18 opportunity.
19 First, I'd like to jump straight to the issue
20 the Court raised just a moment ago is how is Smith
21 versus Maryland distinguishable in this case. It's
22 quite simple, your Honor.
23 In Smith versus Maryland, we had a specific
24 instance of a criminal investigation. There was a
25 criminal who was alleged to have made phone calls to

1 victims and witnesses threatening them, which the police
2 were investigating.
3 Distinguish that from today's case. Today's
4 case you have all of the metadata collected in the
5 United States from the phone service providers before
6 there's any suspicion of any criminal activity of
7 probably 99.9 percent of those individuals whose data is
8 collected.
9 Let's apply those facts to Smith versus
10 Maryland. If, in Smith, the police or the government
11 had gone out and collected every single telephone
12 metadata before they ever had any suspicion of Smith,
13 perhaps even before Smith had even committed a crime,
14 put that into a database, held onto it, then learned
15 maybe Smith was up to something and searched that data
16 and found out he had made calls to certain individuals.
17 Smith turned on a criminal investigation that
18 happened before there was a collection of the data. In
19 other words, the reasonable articulable suspicion that's
20 set forth in the statute which the government must have
21 to query existed before they even possessed the data.
22 And, moreover, Smith versus Maryland involved a pen
23 register that was installed on the government's phone
24 system, not a mass data dump as we have here.
25 The Court mentions the time periods that have

1 gone by --
2 THE COURT: Just a moment. You say that Smith
3 v. Maryland involved a collection of data from a
4 government? Did I miss --
5 MR. SMITH: The government installed the pen
6 register on the phone company's system to collect the
7 data.
8 THE COURT: But with the -- I mean, in
9 coordination with the telephone company?
10 MR. SMITH: Correct.
11 THE COURT: How do you deal with the
12 Van Leuven case and the other cases from the Supreme
13 Court and the Ninth Circuit suggesting that simply
14 ceasing like envelopes or mail without actually
15 examining their content does not create a fourth
16 amendment issue, isn't that really a close parallel to
17 what happens here?
18 Unless there's some evidence that, in fact,
19 something happened more than collecting the -- I want to
20 use this word telephony, I think is the correct
21 pronunciation, telephony metadata.
22 MR. SMITH: Correct, your Honor. The envelope
23 cases and the suitcase cases, which involved a dog
24 walking by a suitcase and smelling narcotics or not
25 smelling narcotics.

1 THE COURT: Right.
2 MR. SMITH: Can be distinguishable from this
3 case because the data being collected here isn't inside
4 of any envelope, it's not inside any case; it is the raw
5 data that is being provided to the government.
6 Therefore, every single day we get a data
7 dump. There's nothing that needs to be done or nothing
8 that needs to be opened to review that data. Simply it
9 needs to be queried and if they had a seed number.
10 THE COURT: Again, the problem we have, and
11 it's my heartburn with Justice Scalia and his
12 originalist view of the world, which I -- I think even I
13 just reread Jones and I think it's pretty clear that
14 Justice Alito and other conservative members of the
15 court are not following that, but we live in a different
16 world.
17 And, today, isn't there a direct analogy to
18 storing metadata on a computer, but not actually
19 reviewing it through search terms? Isn't there a direct
20 analogy between that and holding an envelope,
21 snail-mail, if you will, and then not -- but not
22 examining the contents? Isn't that the 21st century
23 analogue to what was going on in Van Leuven and those
24 cases?
25 MR. SMITH: With all due respect, your Honor,

1 I disagree with that assessment.
2 THE COURT: I'm just asking, I'm not -- so
3 don't --
4 MR. SMITH: The -- the envelope analogy you
5 actually have to take something, open it up to read
6 what's inside of it. Okay. A human being does that in
7 all likelihood because we can't have a computer open an
8 envelope and look at the letter.
9 Here we have the data, which is raw data, that
10 is put into a database and then queried by a computer.
11 And perhaps what the Court is getting at is we don't
12 have an actual person looking at Ms. Smith's --
13 THE COURT: Well, no, you don't need to have
14 an actual person look at it; a computer can do that
15 function for you. But I guess what I'm saying is, isn't
16 running the query, the 21st century analogue to opening
17 the envelope?
18 MR. SMITH: No, your Honor.
19 THE COURT: Okay.
20 MR. SMITH: It is certainly not. Because once
21 you run the query, it has to go through -- from what I
22 understand of the system, it runs through the numbers
23 that that phone number may have called. And to do that
24 it must open up the data that it received from the
25 telephone company every single day.

1 And I believe that the data that's delivered
2 on a daily basis isn't in some sort of suitcase or in
3 some sort of envelope, it is the raw data.
4 THE COURT: Okay. Now, maybe we're not
5 communicating. I want to make sure I understand, and
6 the government may want to listen carefully and correct
7 me where I'm wrong because I'm sure I'm wrong on some
8 aspect of this.
9 But my understanding was that if queries were
10 run on telephone numbers which were a certain number of
11 jumps from a target, someone identified as a potential
12 terrorist organization. And that if unless you were
13 within that number of jumps, even when queries were run,
14 the queries were so limited so that you would not
15 actually be focusing on in any way particular metadata
16 unless you were within that connection.
17 Now, I could be dead wrong on that issue, but
18 were you assuming that the way I characterized it is the
19 way it operated? Or at least thinking when they run a
20 query it's on the entire database of every telephone
21 call made in the United States?
22 MR. SMITH: I think I'm following what your
23 Honor is stating. And the way I understand it to
24 operate is there is a seed number, which is a number of
25 a known person of interest.

1 THE COURT: Correct.
2 MR. SMITH: That number is entered into the
3 database. That number and every number it possibly
4 could have called or did call are returned as --
5 THE COURT: Not every number it possibly could
6 have called because that's the entire universe, so it
7 has to be the numbers they actually did call, correct?
8 MR. SMITH: It searches the database for the
9 numbers that that number called.
10 THE COURT: Okay.
11 MR. SMITH: And to do that it has to go
12 through the numbers that may have received the call to
13 cross-reference them, does that make sense?
14 THE COURT: All right.
15 MR. SMITH: Then that is the first hop. You
16 get numbers from that that they called. And until
17 January of this year they had three hops.
18 So we would take all the numbers that were
19 returned in that query and find out who called them or
20 they called, which gave us another universe of numbers,
21 and then that would be searched to see what numbers
22 called or they called on those numbers. Those were the
23 three hops.
24 But to get the correlation of numbers that
25 you're looking for to see who called who, there must be

on the one side of the equation all the phone numbers out there that are in the database, what numbers did they call, plus the numbers that were part of the seed number or the hops, what numbers did they call or receive a call from.

So in order to run a search of the database, you must search every number that could possibly be in there to make sure that those numbers are not covered by the query.

THE COURT: Well, so -- so you're suggesting that even if you're not within three hops of a seed or target number, even if that's not true, your Fourth Amendment rights have been violated simply by the possession of the telephony metadata and subjecting this entire universe of telephone data collected to this search to determine who is within three hops of the seed or target?

MR. SMITH: That would be correct, your Honor. That's exactly our position is that every query is a search of the plaintiff's phone number to see if they correlate with the seed number, a hop number or a hop number.

THE COURT: Well, how -- let's, again, try to go back to the 20th century -- or the 19th century analogue. If you have a file cabinet full of data --

1 full of envelopes that have been seized. And over time
2 it's held and then there's a reason to go back and
3 review it. Simply thumbing through and looking at the
4 number, the address, the addressee, the addresser, is
5 that a violation of the Fourth Amendment given
6 Van Leuven?
7 MR. SMITH: Looking at the outside of the
8 envelopes?
9 THE COURT: Right.
10 MR. SMITH: Under Van Leuven it would not
11 because you're simply looking at the outside of an
12 envelope, your Honor. You're not looking at --
13 THE COURT: See, that's what I'm wondering.
14 Why is that -- again, we have to work with analogous,
15 and maybe that's not the best word, but it's the best
16 word I can come up with to try to -- because technology
17 changes so fast that even the things we talked about ten
18 years ago may be -- is not -- maybe are not relevant
19 today.
20 But isn't that roughly what is going on here
21 albeit electronically?
22 MR. SMITH: Two things, your Honor.
23 First, the scope of the search of (inaudible)
24 phone numbers if it's queried is much greater than the
25 scope of just looking at a file cabinet of envelopes.

1 I think Judge Leon made the analogy that going
2 to a library and looking at books and seeing if books
3 were in the library is totally different than seeing if
4 a certain cite was within every single book, so you have
5 to open every book to actually look at it.
6 And I think the envelope analogy doesn't
7 necessarily apply to this case directly because the data
8 is not contained within anything other than a database
9 which can be queried at any point in time --
10 THE COURT: Okay.
11 MR. SMITH: -- by the government. It's being
12 stored by them. It's not looking at the outside of an
13 envelope. You're already inside of the envelope. The
14 data is there to be run and reviewed, and so the
15 envelope analogy or the suitcase analogy I don't think
16 fits with this because you're taking data from the phone
17 company and putting it into the database and it's
18 querying it.
19 THE COURT: And I think that's an excellent
20 response because to be truly analogous, you need to
21 actually review the contents of the letter as part of
22 the thumbing through, but what that then raises is the
23 fact that unlike a letter this -- we're essentially
24 collecting -- or the government is essentially
25 collecting only the addresser and the addressee of that

1 envelope.
2 So the data actually being reviewed is not the
3 contents of any actual communications, it's the fact of
4 the communication, who it was addressed to and who it
5 was addressed from. So if Van Leuven's not a problem
6 then maybe then we're back to having kind of a Jones --
7 or Smith problem rather, a Smith problem.
8 MR. SMITH: A reasonable expectation of
9 privacy that society accepts, of course, your Honor.
10 And getting back to Smith and the data that's
11 being collected and reviewed. The data is phone numbers
12 called, phone calls received --
13 THE COURT: Length of the call.
14 MR. SMITH: -- length of the call and the
15 trump data. And if you read the Feltman affidavit which
16 was filed in a sister case to this one, he talks about
17 what the trump data really is. The trump data is an
18 identification of where the call was made from, so
19 there's some location data in this information as well,
20 which I think takes us outside of the Smith scenario
21 because Smith was locked.
22 I mean, Smith was -- he called from his house,
23 they got the number he called. In this case, we have a
24 cell phone. They can tell from the trump data if it was
25 made from California, Hawaii or Kansas. So we got an

1 expansion of the data that is available, and I think
2 that affects the reasonable expectation of privacy.
3 Moreover, your Honor, you have cell phones in
4 this day and age which can really paint a great picture
5 of what a person does, who they affiliate with.
6 THE COURT: You know, I read that in the brief
7 and, of course, what I am concerned about is -- with
8 that argument is if indeed what is being collected is
9 not telephony metadata but rather accessing your Google
10 or Bing or whatever your search engine is, reviewing
11 what it is that you're looking at, or if it involves
12 your e-mail communications or if it involved what movies
13 you were watching. This would be a very different case.
14 But if it is only telephony metadata, isn't it
15 just Smith v. Maryland type information? That's what
16 I'm worried about. It's very easy to just say, well,
17 smart phones do so much more. But if what they do that
18 is relevant here is just telephone calls, who was
19 called, the length of the call, and who -- who was being
20 called, it's a somewhat expansion of Smith because I
21 think Smith was just who was called, but it's not that
22 much more.
23 I mean, we're not talking about -- I mean, I
24 would truly agree that the sky is falling if everything
25 on my cell phone is now being reviewed by the

1 government. That's a whole different matter though. Or
2 am I wrong?
3 MR. SMITH: You're not wrong. It is an
4 expansion of Smith, but it's not as you said the sky is
5 falling.
6 THE COURT: Okay.
7 MR. SMITH: We don't know for a fact that
8 e-mails are being reviewed or stored. We don't know for
9 a fact the scope of the program as far as content is
10 concerned. Frankly, because that hasn't been revealed.
11 THE COURT: Let me address that issue very
12 quickly and this will be -- I'm sure Ms. Berman is going
13 to argue there's a lot of assumptions here. Well, the
14 reason there's a lot of assumptions is the plaintiffs
15 have no way of knowing and no way of accessing the
16 information because of national security concerns.
17 So I'm going to look a little bit jaundiced --
18 or have a jaundiced eye in looking at any argument that,
19 you know, Verizon, there's no evidence that Verizon has
20 actually has provided their information.
21 There's no way in the world the plaintiffs
22 could ever determine that, but there's certainly enough
23 indicators in the public domain in terms of statements
24 being made to draw a broad -- that would allow one to
25 draw that inference. I would, for purposes of our

1 argument here today, I would really like to focus on
2 what I think are reasonable assumptions, and I know
3 Judge Leon made those assumptions, perhaps he should not
4 have, perhaps the record didn't support it.
5 But I think the plaintiffs in a case like this
6 are in a very difficult position because they have to
7 fight essentially with at least one arm, maybe both
8 arms, tied behind their back.
9 Go ahead. I just wanted to head that argument
10 off at least for purposes of today's argument.
11 MR. SMITH: Certainly in getting back to Smith
12 versus Maryland distinguishing factors.
13 Again, I'm going to go back to the start of
14 how I believe that Smith is very different and the
15 Miller case, which was decided three years earlier. And
16 that is, the data is being collected before any
17 suspicion or investigation is really started as to
18 Ms. Smith. She is not a criminal suspect. She is not
19 suspected of anything, but all the data is being
20 collected. You go back to Miller.
21 Miller involved bank records; checks, deposit
22 slips, financial statements, that the government wanted
23 and is part of a criminal investigation. If Miller were
24 this case, what would have happened is the government
25 would have taken all of that data, prophylactically,

1 before it was ever needed and put it in a database and
2 then caught Miller and said, Let's run his information
3 through our database, which we've collected, and see if
4 we come up with anything. And what do we learn about
5 that person?
6 And I think if the Supreme Court was faced
7 with that decision, it would clearly state, in my
8 opinion, that it's distinguishable. And if you take
9 Smith versus Maryland, it's the same deal. It was a
10 13-day wire tap or pen register on the phone. It was a
11 limited period of time. Mr. Smith was already under
12 suspicion.
13 If that were applied in this case, what the
14 government would have done is never needed the pen
15 register. It would have simply collected all the data,
16 put it in his database, picked up Mr. Smith and then run
17 his information through the database to see if it was
18 relevant. I think those facts distinguish Smith versus
19 Maryland and the Miller case from our current situation.
20 What we have here is we have the government
21 saying, We believe we have the authority under statute
22 and the Fourth Amendment to go out and gather
23 information from nearly every single American without
24 them ever knowing about it. We would not be standing
25 here today unless somebody broke the law, in my opinion.

1 But we are standing here today because we learned that
2 they are gathering this information, storing it for five
3 years and if something comes up where they think this
4 person may be connected to someone or not even think
5 that, have a suspect and run that number, and then
6 somehow maybe misdialed the plaintiff's number. All of
7 a sudden her number shows up on that list and then all
8 the numbers she dialed show up on that list.
9 It's analogous to doing a drug investigation
10 and going out and saying, I'm going go search this house
11 for drugs and then finding that guy's cell phone there,
12 finding all the numbers and then searching everybody
13 else's house to see if they have paraphernalia as well.
14 The scope with which we have an investigation
15 here pre any reasonable suspicion of criminal activity
16 is the problem with the Fourth Amendment. If we live in
17 an age today where the government can collect data and
18 just sit on it and then wait to run searches, I think
19 that's a violation of the Fourth Amendment.
20 And then if you consider where we're headed in
21 this case, and I hate to talk about a slippery slope,
22 but the argument under Smith is it's data that you
23 provide to a third party, so therefore you have no
24 reasonable expectation of privacy.
25 Well, any data that I provide to a third party

1 then would be outside the scope of the Fourth Amendment.
2 For example, I run with a Nike GPS app. It provides
3 location data to Nike. What stops the government from
4 asking Nike, in secret, for my location data. And once
5 we start down this road of gathering data ahead of time
6 just because we may need it, we're certainly going into
7 the realm of a Fourth Amendment violation. And I don't
8 think it's something that the founders of our country or
9 the Constitution supports.
10 Now, we have to balance that, obviously. I'm
11 not ignorant to the balancing that we must do for
12 national security. And I think the president stated it
13 well in his speech in January of this year where he said
14 a possible solution would be to have the third parties
15 maintain the data, then we get a suspicion. The
16 government has a suspicion about an individual and they
17 go to the phone company and they say this is the number
18 of a known or a suspected terrorist, give us the hops.
19 I don't believe that violates the Fourth Amendment.
20 Because we're not gathering all the data
21 before we have some sort of suspicion. But in this case
22 what distinguishes it from all the jurisprudence that
23 came before it is that we're gathering data, the
24 government is gathering data before it has any suspicion
25 of the people it's gathering data on.

1 And we all know as President Obama said in his
2 speech and I cited in my brief, it's not enough just to
3 say trust us. Trust us with the data that we collect.
4 I believe the Fourth Amendment provides individuals
5 within this country that are just going about their
6 lives a reasonable expectation that everything they do
7 will not be collected by the government and in this case
8 I only know about phone numbers dialed, phone numbers
9 received, length of call and trump data. I believe that
10 is even more data than what the government should be
11 entitled to.
12 Under Smith versus Maryland, the Miller case
13 and all subsequent cases. Because in those cases they
14 are clearly distinguishable. You do not have this going
15 out to a third party and asking them for data related to
16 a suspect. This is gather everything and then we'll
17 find out what we need at some later date. And I believe
18 that distinguishes -- I don't think the U.S. Supreme
19 Court has ever addressed a question of this magnitude
20 where the government is out there collecting data on --
21 according to the Washington Post and the Wall Street
22 Journal -- over 99 percent of Americans.
23 And you talked a little bit about the standing
24 issue, but I would like to point out that the most
25 recent submission of the order that was entered by the

1 FISC mentions -- blacks out all the names of the
2 cellphone provider that challenged the search under the
3 Klayman case.
4 But the Washington Post reported on August --
5 April 25th, 2014, that it was filed by Verizon. And it
6 would be amazing to believe that this program in this
7 comprehensive database which is so necessary to protect
8 us would leave out the largest wireless carrier in the
9 United States.
10 Now, do I have facts to support that? Do I
11 have a document I can hold up and say, your Honor,
12 they're collecting from Verizon? I do not. But at this
13 stage how do I get it? I can't.
14 It either is going to get leaked or it's going
15 to be authorized to be declassified. But I cannot
16 believe as the judge in the Klayman case mentioned that
17 we have all this argument about how comprehensive the
18 database is and how it provides so much security and
19 then at the same time say, oh, by the way, we missed all
20 of these calls.
21 So on the standing issue, your Honor, I kind
22 of diverged back into it, but I just wanted to point
23 that out that I believe now as we are learning more
24 information through press and otherwise that every cell
25 phone provider in the United States, every call made on

1 every network, is at least caught somehow. Whether it
2 be directly from their service or if they have to jump
3 from tower to tower. Because I think there's
4 information in the record about if you make a call and
5 you jump onto an AT&T tower, it makes no difference. It
6 still gets picked up. Or you jump onto a Verizon tower
7 or Sprint tower.
8 And if you look at the more recent news
9 reports, and I think they came out yesterday, about the
10 Sprint challenging the actions of the government back in
11 2009 and 2010. They didn't actually go to court from
12 what I understand, but the justification for the program
13 was released and after that, as late as 2013, the FISC
14 was saying nobody ever challenged this conduct, which I
15 believe is a little bit of a technicality in the sense
16 that it may not have been challenged in court, but
17 certainly these providers are looking into it.
18 But, your Honor, back to the Smith versus
19 Maryland distinctions. If the government is allowed to
20 gather all of this data and I think there's substantial
21 evidence in the record supporting that the picture that
22 can be painted of an individual as a result of all that
23 information is quite detailed. Especially when you look
24 at five years of data.
25 I think the act of simply collecting it ahead

of time from third parties and then saying this is just like Smith versus Maryland, doesn't carry any weight.

And unless the Court has any other questions for me --

THE COURT: No.

MR. SMITH: -- I would say the Court should grant the motion for preliminary injunction and deny the motion to dismiss.

THE COURT: All right. Thank you very much.

Ms. Berman.

MS. BERMAN: Good morning, your Honor.

Let me address the matters that the Court raised and that Mr. Smith raised.

First of all, this case is absolutely foreclosed by the Supreme Court precedent of Smith versus Maryland. Your Honor is absolutely right that that holding there that there is no reasonable expectation of privacy in the phone numbers dialed even if you believe that the phone company is going to keep that information confidential, that holding is squarely applicable here.

THE COURT: Let me ask how -- I'm trying to think how Jones affects this and this really is a play off from Mr. Smith's argument here that it's the magnitude of the process. The magnitude of the

1 collection of the data that is problematic. The Jones
2 case, even though as you point out in your brief, you
3 know, it was an odd mix of justices, with as I recall
4 Justice Scalia writing an opinion for I think four
5 judges -- four justices himself, Thomas -- I'm drawing
6 a -- the Chief Justice Roberts and Justice Kennedy, if
7 I'm adding it up correct, Justice Sotomayor wrote a
8 concurring opinion and then there was a concurring in
9 judgment opinion by Justice Alito joined by Breyer,
10 Kagan and Sotomayor if I've got that right.
11 It seemed quite clear to me that the four
12 justices who sign onto Justice Alito's view had some
13 real concerns that the use of GPS monitoring for an
14 extensive period of time and tracking all activities,
15 that that really made a difference and that that
16 distinguished it from earlier decisions saying that GPS
17 monitoring really did not create -- did not violate an
18 expectation of privacy because what a person does, where
19 you drive in your car is something you can see, anybody
20 can see.
21 What I'm concerned with is the tenor of Jones
22 may suggest that Smith -- that the Supreme Court might
23 view Smith quite differently if instead of a focused
24 individualized, what's the term, not trap -- well, pen
25 register, that a short-term pen register that that might

1 be viewed very differently if what we have is a
2 collection of every phone call you've made for five
3 years and the ability, albeit not -- and that's where
4 maybe Miller comes into play, but at least the
5 collection of that volume of data may be looked at very
6 differently by at least those four justices and possibly
7 Sotomayor as well because it seemed to me she was on the
8 fence on that issue, was really saying we just don't
9 need to go there because clearly we have the trespass
10 and even under pre-Katz law that was enough. So help me
11 out with that.
12 Do you understand where my concern is?
13 MS. BERMAN: Yes.
14 THE COURT: I'm not sure I'm being very
15 articulate.
16 MS. BERMAN: Yes, your Honor. You're being
17 perfectly clear.
18 What I would say in response is that Justice
19 Alito's concurring opinion in Jones is all about
20 location and movement and the ability to track
21 somebody's movements and locations and the privacy
22 implications of that.
23 We don't have that here at all. This program
24 does not involve monitoring by the government of
25 people's movements. And the -- one of the FISC opinions

1 that we cited in the record, we provided in the record
2 at Exhibit D, the October 11, 2013, opinion says that at
3 page 5.
4 So, first of all, we're not dealing with
5 location, we're not dealing with tracking people's
6 movements, and that's what Justice Alito was primarily
7 concerned about.
8 Second of all, Jones was not a third-party
9 doctrine case. In Jones, the police surreptitiously
10 attached the GPS device to Mr. Jones' car and tracked
11 his movements through the GPS device for four weeks, I
12 believe.
13 So there was no question in that case that
14 Jones had not voluntarily conveyed or exposed or turned
15 over that information to the police. Jones doesn't
16 involve the third-party doctrine at all. It was decided
17 on the narrowest possible grounds of the trespassory
18 doctrine and the, you know, the Court relied on the
19 physical intrusion that the tracker affected, and
20 specifically declined to address the question of whether
21 the use of the GPS device impinged on a reasonable
22 expectation of privacy.
23 THE COURT: No, I understand that.
24 MS. BERMAN: It had nothing to do with
25 third-party doctrine at all.

1 THE COURT: Completely agree that's what the
2 Court did. And it was Justice Sotomayor that became the
3 critical decision because the sense was that she, as I
4 think most judges should, we should decide cases on the
5 narrowest ground possible. And she said we don't need
6 to go there, but four of the justices did go there and
7 said no this is a Katz violation of an expectation of
8 privacy case once you are involved in long term or
9 expanded activity. And that's why I'm concerned that
10 that same four justices plus maybe Sotomayor may say,
11 you know, maybe Smith doesn't really apply here because
12 this is, again, an expansion of what we were dealing
13 with in Smith.
14 MS. BERMAN: Right. So, your Honor, I think
15 the other really important point about Jones and
16 particularly Justice Sotomayor's concurrence is that the
17 concerns are that -- expressed were that by tracking a
18 person's location and movements for an extended period
19 of time, it reveals a wealth of personal information
20 about their life. Okay. And that is because of the
21 individualized nature of the government activity there.
22 Where, again, the police attached the GPS to
23 his car. They know whose car it is. They suspect him
24 of some criminal activity and they are tracking him.
25 And they associate the GPS information they get back

1 with him. They map out what he's been doing for four
2 weeks and they actually use that information to arrest
3 him and prosecute him and send him to jail.
4 And the same thing happens in Smith, your
5 Honor. Okay. Again, there you have a pen register. It
6 is used against a known individual and they use that
7 information to arrest, prosecute and send him to jail.
8 Okay. You don't have that in the telephony metadata
9 program.
10 Where the -- the information, the telephony
11 metadata that comes into the government's hands does not
12 contain any identifying information. It comes as raw
13 numbers and, you know, there's no subscriber have
14 information this there and, again, that's not just trust
15 us. Those are FISC orders that are rigorously enforced
16 by a whole web of audits and reporting, compliance,
17 oversight by multiple agencies and branches of
18 government.
19 Okay. So the information doesn't come in with
20 any subscriber identifying information; not name, not
21 address, nothing. And then, again, by virtue of the
22 FISC orders, the NSA can only find out that information
23 in connection with a phone number that is the result of
24 a query. And, again, your Honor, you nailed it before
25 about how the query process works.

1 The government has to have reasonable
2 articulable suspicion that a particular phone number is
3 associated with a foreign terrorist organization that is
4 the subject of an FBI investigation. If it does, if it
5 makes that showing, and it takes that number and the
6 computer queries the database with that number and
7 returns phone numbers that are connected either one step
8 or two step now from that original seed number.
9 And it's only within that population of query
10 results that the NSA is permitted to use other
11 information it has or open source information to
12 determine who a phone number belongs to.
13 THE COURT: Okay. Now, let me ask. What if
14 Ms. Smith in this case had tangible evidence that she
15 was within that second hop of a seed and therefore her
16 phone records had, in fact, been subjected to this
17 heightened or increased scrutiny.
18 How would that change the case?
19 MS. BERMAN: Your Honor, I think it actually
20 wouldn't change the case. Because in Smith itself --
21 Smith itself recognized in the dissents that phone
22 numbers -- that a phone number that you dial can have
23 all sorts of personal information in it and can tell you
24 something about a person's life, and the Supreme Court
25 still held -- that was in the dissent in black and

1 white, the Supreme Court still held that there was no
2 reasonable expectation of privacy in collecting metadata
3 because it's voluntarily conveyed to the phone company.
4 And you assume the risk when you convey it that the
5 phone company is then going to turn it over to the
6 government.
7 And, your Honor, this is -- Mr. Smith
8 mentioned Miller. This is not just the Smith versus
9 Maryland case. That's obviously our best case because
10 it's directly on point, it's the same exact kind of
11 information. But Miller, all these cases before it,
12 dealt with much -- records of a much more personal
13 nature than just telephone numbers dialed.
14 Miller was four months of customer bank
15 records, copies of checks, deposit slips, financial
16 statements, monthly statements, very personal
17 information. Another case that the Smith court cites
18 the Couch (phonetic) case, was tax records from an
19 accountant. You know, a person who went to an
20 accountant for the accountant to do his taxes and all
21 this personal financial information the accountant is
22 required to turn over, not because it doesn't reveal
23 something about the person's life but because the person
24 went to the accountant knowing that, you know, he was
25 turning over that information to the accountant.

1 So there's -- there's a long line of cases
2 here in this third-party doctrine that are -- that
3 are -- involve more personal information and that are
4 just rock solid ever since, you know -- there's
5 nothing -- there's nothing but -- no one's overruled
6 them, they're very good law.
7 Your Honor, if I could turn to what Mr. Smith
8 really was focused most on I would say, which was his
9 contention that in Smith versus Maryland, Mr. Smith was
10 suspected of a crime whereas here the metadata is
11 collected without individualized suspicion of a crime.
12 First of all, all the cases do not analyze
13 that at all. It's -- the question is does anybody,
14 whether you're suspected of a crime or not, have a
15 reasonable expectation of privacy in the information?
16 And the individualized suspicion factor goes more to the
17 reasonableness of the search once you find that there's
18 been a search even the claimant opinion looks at it in
19 that framework.
20 And I would also really like to point out that
21 two of the cases that we cited in our brief on page 21
22 the Dionisio case, I'm not sure if I'm pronouncing that
23 correctly, and the In Re: Grand Jury case. We cited
24 both of these cases in the argument about why the bulk
25 collection of the metadata doesn't -- is irrelevant to

1 whether or not Smith applies.
2 But in both of those cases, you had people who
3 were -- who had conveyed information to third parties
4 who weren't suspected of any crime whatsoever and they
5 challenged subpoenas for that information that they had
6 turned over to the third party.
7 And the courts in these cases in the Dionisio
8 case, it's the Supreme Court, and the In Re: Grand Jury
9 case it's the Eighth Circuit. Both of those courts held
10 there was no reasonable expectation of privacy under the
11 third-party doctrine.
12 So it's not -- it's just simply not true as
13 Mr. Smith said that this is the only -- that this really
14 distinguishes this case from all these other cases. In
15 the Dionisio case, it was a grand jury subpoenaed voice
16 exemplars from 20 people in order to compare against a
17 voice recording that the grand jury had in its
18 possession.
19 And one of those 20 people who -- totally
20 law-abiding person who had done nothing but go around
21 and talk in public challenged that grand jury subpoena.
22 Again, the Court said you expose your voice every day to
23 the public, it's not protected. There's no reasonable
24 expectation of privacy under the third-party doctrine.
25 In the In Re: Grand Jury case that we cite,

1 the Eighth Circuit case, that was a subpoena to Western
2 Union for a whole batch of its wire transactions and
3 Western Union in that case challenged the subpoena on
4 behalf of its customers. And they said, look, you're
5 going to get information from all these innocent people.
6 They've done nothing but use our services.
7 And, again, the Court said, well, they are
8 voluntarily conveying that information to you, the
9 information about what, you know, how much money they
10 need and where they're sending it to and when. They're
11 conveying that to Western Union and so Western Union has
12 to convey it to the government.
13 So I think those are two cases that really go
14 to Mr. Smith's argument on that point.
15 Your Honor, I would just like to next address
16 the argument about the telephony metadata, the fact that
17 this is the same exact kind of information at issue in
18 Smith. The other data that's collected here, the dates
19 and times and durations of the call that were not, you
20 know, at issue with the pen register, that again is also
21 voluntarily turned over to the phone company or
22 generated by the company itself.
23 So if it's squarely within the rationale of
24 Smith even though it's a slight divergence from the
25 facts, it's -- the rationale applies squarely to those

1 other types of metadata. And, in fact, FISC recently
2 found in the opinion that we submitted to you
3 beginning -- I believe at the beginning of last week,
4 the March 20th opinion, found that the pen register data
5 at issue in Smith was, quote, undistinguishable from the
6 metadata involved here.
7 Again, the United States versus Reed case that
8 we cite in the brief is the Ninth Circuit talking
9 about -- saying that because data about call
10 origination, length and time of call is, quote, nothing
11 more than pen register and trap and trace data, there is
12 no Fourth Amendment expectation of privacy citing to
13 Smith. That's the Ninth Circuit.
14 And in the Moalin case that we also cite in
15 the brief, the Court holds there that there's no
16 reasonable expectation of privacy in the receipt of call
17 data from a third party. And, the Smith reasoning
18 applies to devices that catch your outgoing call
19 information.
20 Your Honor, next I'd like to address the
21 argument that times have changed. That time and
22 technology are different now. We have cell phones.
23 Everybody walks around with a telephone in their pocket
24 and they use it for all sorts of things that couldn't
25 have been imagined in 1979.

1 Well, your Honor, the phones back then were
2 surely as personal for all sorts of -- were used for all
3 sorts of personal purposes. I think I alluded to this
4 before that this Justice Stewart's dissent in Smith
5 recognized that lists of phone numbers dialed, quote,
6 easily could reveal the identities of the persons and
7 the places called and thus reveal the most intimate
8 details of a person's life.
9 So telephones were used for this same purpose
10 back then as they are now.
11 THE COURT: But you would agree that if the
12 metadata being collected included what images -- what
13 photographs I took, what images I brought up using
14 Google, what searches I conducted, what websites I
15 visited, somehow that -- wouldn't that change or at
16 least cause us to start scratching our head to try to
17 figure out how Smith might apply if the data being
18 collected is that much more substantial?
19 MS. BERMAN: Your Honor, it might. It is not
20 at issue here.
21 THE COURT: I understand that -- you can make
22 the very same argument, I voluntarily exposed that
23 information to the rest of the world. To (inaudible) in
24 the case of my personal, as it is Surface Pro or
25 whatever it is I'm using, not only Verizon which happens

1 to be my carrier, but my employer, anybody who has
2 access to this, I'm exposing myself to the world and my
3 conduct to the world when I do this or the same argument
4 can be made.
5 But doesn't the change of the way we interact
6 with the world and the fact that instead of reading --
7 you know, I dropped by subscription to my local
8 newspaper years ago and I read it online. Well, does
9 the fact that I now use a media which allows somebody to
10 look at what I'm reading and know what it is I read
11 change the dynamics so that I don't have an expectation
12 of privacy about what I read but when I was reading just
13 books that I ordered and had in my personal library, I
14 did have an expectation of privacy. Don't we have to --
15 MS. BERMAN: Your Honor, I think that one
16 thing that is important about Smith is that the Court in
17 deciding that there is no reasonable expectation of
18 privacy and information turned over to the phone
19 company, the Court said part of that analysis is that
20 people understand -- everybody in that day and age in
21 1979 understood that the phone company had the
22 facilities to record that information and did, in fact,
23 record it in those cases.
24 You know, in the bill -- you got a bill that
25 itemized the calls that you made and everybody also it

1 was common knowledge that it was used for fraud
2 detection purposes. So I think you would all -- in the
3 various hypotheticals that you're talking about I think
4 you would have to know the particulars of that and the
5 extent to which that information is being recorded and
6 the extent to which people understand that. And, again,
7 those are the hard cases and we -- we don't have that
8 here.
9 THE COURT: We don't have it. I am just
10 speculating here. But I fear that we'll reach a point
11 that so much of our interaction with the world is
12 electronic and therefore because it is electronic it's
13 subject to review by whoever our carrier is, whoever
14 other individuals that we soon will have no expectation
15 of privacy unless we live under a cone of silence on a
16 desert island, and at some point we have to maybe
17 redefine what we need by an expectation of privacy.
18 I'm not going to be the one to do that, I
19 might add. That's up to the Supreme Court. I'm not
20 that gutsy. But I do feel that the Supreme Court or
21 someone is going to have to really take a hard look at
22 what -- whether or not revealing this kind of
23 information to third parties doesn't change the fact
24 that we still have an expectation of privacy. But case
25 law is what it is and I'm not going to be the one to

1 upset that.
2 MS. BERMAN: Right. Exactly. That's for the
3 Supreme Court to do.
4 And I would also just point out that it's
5 interesting in the Smith dissents -- in both dissents,
6 in Justice Marshall's dissent and Justice Brennan's
7 dissent they make this point, too, back in 1979
8 telephones weren't necessary to conduct the affairs of
9 modern life.
10 Justice Marshall said phones have become a
11 personal and professional necessity. And Justice
12 Brennan said the necessity having a bank account -- it
13 talked about the necessity of having a bank account to
14 participate in modern economic life. So they made these
15 points back then and, you know, I think those cases do
16 demonstrate, Smith was using the phone to harass
17 somebody. And, you know, Miller it was all sorts of
18 personal records that, you know, someone had a bank
19 account and needed a bank account back then just like
20 you do now.
21 THE COURT: It becomes more pervasive and it
22 becomes more impossible for someone to drop out, so to
23 speak, you know, to do a Ted Kaczynski and move into
24 your cabin in the Montana forest. If that's the only
25 option we have, then I think maybe we have to reevaluate

1 where we are. But that's -- that really does not affect
2 this case. It's clearly relevant, but it doesn't change
3 what we're dealing with here today.
4 Go ahead.
5 MS. BERMAN: Okay. Just to hit on another
6 point that the argument that the program collects
7 metadata related to a large number of other people's
8 calls isn't relevant. I discussed this a little bit in
9 talking about the Dionisio and In Re: Grand Jury cases,
10 but the FISC just recently stated in its March 20th
11 opinion that this argument is misplaced under settled
12 Supreme Court precedent and they're talking about the
13 (inaudible) line of cases which holds that Fourth
14 Amendment rights are personal in nature and can't bestow
15 vicarious protection on those that do not have a
16 reasonable expectation of privacy in the place to be
17 searched. And, again, we cite these cases in our brief
18 where there was a large volume requested and the courts
19 held that that was irrelevant.
20 And also the Moalin case that I mentioned,
21 actually applied this principle to the telephony
22 metadata program when it said that the defendant
23 couldn't complain about the government's use of metadata
24 about calls between third parties under this principle
25 that Fourth Amendment rights are personal.

1 Your Honor, if I could, I would like to
2 address the questioning about the computer search and it
3 being in the 20th century analogue to the Van Leuven
4 cases. I think that's absolutely right and it is
5 another factor here.
6 I mean, we absolutely think that Smith is --
7 forecloses the claim that there was a search at all, but
8 there also wasn't a search because the government
9 never -- they, you know, Ms. Smith can't show that her
10 metadata or metadata related to her calls was ever
11 looked at or analyzed by the NSA.
12 And while it is in that database, there is
13 no -- nobody analyzing it unless it's within two hops of
14 the suspected terrorist selector and there's no evidence
15 whatsoever that any of her calls would fit that
16 description.
17 THE COURT: But, of course, how would they
18 know? You know, I -- I mean, unless you're --
19 MS. BERMAN: Well, she's not alleging it.
20 THE COURT: -- Alicia Florrick on The Good
21 Wife and it happens that the Governor -- I mean, there
22 was an episode dealing with this very issue of that TV
23 show some time in the last year or so. And unless you
24 happen to be in the circumstance where somehow it
25 fortuitously falls in your lap, you would never know

1 that you were within two hops of a -- or three hops, up
2 until a year ago, of a seed.
3 So I -- that's one of the challenges. And I
4 understand that's maybe the way life works, but that is
5 of concern that if a person has, in fact, their rights
6 have been violated and I suppose you might argue if
7 they -- no harm, no foul; if they don't know it, then
8 presumably there's no injury. But I don't think we want
9 to require concrete injury before the Fourth Amendment
10 kicks in.
11 MS. BERMAN: Your Honor, this Shay (phonetic)
12 declaration, the NSA declaration that we submitted, does
13 say that only a tiny fraction of the metadata in the
14 database is ever reviewed by an analyst. So it's --
15 it's a very small amount and she hasn't made any
16 allegations to suggest that she's in one of them.
17 THE COURT: Okay.
18 MS. BERMAN: And then, you know, also on this
19 point, you know, your Honor was absolutely correct in
20 your understanding of how the -- of the query process
21 and that it's done by a computer. It's all done
22 electronically. And that no human ever sees the
23 metadata associated with anyone's calls unless the
24 number falls within two hops now of the selector.
25 And so it's unlike the library example where a

1 human being is going into the library, reading each and
2 all of those books to find the reference to the -- I
3 forget what Judge Leon used, but --
4 UNIDENTIFIED MALE: Battle Cry of Freedom.
5 MS. BERMAN: Battle Cry of Freedom, thank you.
6 So it's not like that situation at all. And last, your
7 Honor, I just would like to mention on the Fourth
8 Amendment issue that even if your Honor were to find
9 that there has -- was a search, you would then have to
10 address reasonableness.
11 And Mr. Smith failed entirely in both of his
12 briefs to address this issue even though we briefed it.
13 And we -- our position is that the metadata program --
14 telephony metadata program fits squarely within the
15 special needs doctrine where individualized suspicion is
16 not required. There is the overall purpose of this
17 program, it clearly is above and beyond normal law
18 enforcement, normal criminal law enforcement purposes.
19 It is to prevent and detect -- I'm sorry, to detect and
20 prevent terrorist attacks and there's a minimal privacy
21 intrusion balanced against the great government interest
22 in identifying a known terrorist operatives.
23 And so we believe that under the
24 reasonableness analysis the claims should be dismissed
25 as well.

THE COURT: All right.

MS. BERMAN: Thank you, your Honor.

THE COURT: All right.

Mr. Smith?

MR. SMITH: Thank you, your Honor. I will be brief.

First, I will go back to the point, if you look at all the cases that were cited, you don't have anything close to what is going on in this day and age with the NSA and the collection of the metadata.

This metadata is being collected prior to any investigation, prior to any suspicion and simply being housed by the government and then they can query it at any point in time.

And I would point out that the government stresses over and over again how many policies and procedures and oversight that must go in to protect the data from a search or a query. That is all well and good, but the act of actually collecting the data about citizens who aren't under any suspicion of a crime whatsoever is where the violation occurs, and how Smith and Miller and all the previous cases can easily be distinguished.

We are living in a new age where every single day I think it's listed as 50 terabytes of data is

1 dropped into a database and kept for five years subject
2 to a query at any point in time if there's reasonable
3 articulable suspicion about the seed number.
4 So we have reasonable articulable suspicion to
5 run the seed number, but what happens in the first hop?
6 What if it's a Dominos this suspected person called and
7 the plaintiff happened to call that Dominos as well? Do
8 we need reasonable articulable suspicion then to see
9 what numbers she called?
10 It simply opens up the universe of numbers
11 that can be searched at any given time and the real
12 issue with the case from a Fourth Amendment standpoint
13 is that this data is being housed by the government.
14 And as President Obama said, you can't just say trust us
15 to follow our procedures and policies with all of this
16 information, which I may point out that Mr. -- Professor
17 Feltman, and his affidavit's in the record, says that
18 you can paint a great detailed picture about an
19 individual citizen based on this data.
20 Getting back to the search question --
21 THE COURT: Well, you can, but getting -- I
22 guess I'll go back to where we started when I said that
23 it seems to me the Smith decision, the Smith v.
24 Maryland, we have to determine why that does not apply
25 here.

1 The Court there said there is no expectation
2 of privacy in the telephone numbers you called. So even
3 if you are within the two hop or two -- yeah, two hops
4 or the three hops of a seed or suspected terrorist, and,
5 in fact, more than just storing the data there is in
6 fact a scan or query run on that information. Doesn't
7 Smith still say that there's no expectation of privacy?
8 And that's -- and even though it may disclose
9 some pretty significant information, you know, what
10 church you attend, what food you eat, et cetera, what
11 interests you have, what friends you have. Clearly --
12 but that was addressed, I think, by the dissent in Smith
13 and was rejected by the majority of the courts. So
14 don't we still just run head long into that brick wall?
15 MR. SMITH: I think, your Honor, you have to
16 consider Smith under the facts under which it was
17 decided.
18 THE COURT: Okay.
19 MR. SMITH: Which was a criminal defendant
20 being looked into for criminal activity.
21 THE COURT: But the Fourth Amendment rights
22 are not limited to just criminals. So doesn't the same
23 analysis apply whether the focus is on an individual or
24 someone for which there's no -- I mean, Smith did not
25 turn on that there was some reasonable articulable

1 suspicion or a terry type suspicion that somehow then
2 authorizes. They just said, no, you don't have any
3 expectation of privacy in this.
4 And doesn't that analysis apply whether you're
5 a criminal or not a criminal?
6 MR. SMITH: Your Honor, if you look at the
7 Smith cases, I'll go back to the distinguishing fact,
8 which I believe is distinguishing all those cases. Is
9 that we have a collection of data, then a running of the
10 search.
11 THE COURT: Okay.
12 MR. SMITH: In Smith and all the other cases,
13 the Supreme Court did not face the situation where the
14 government had, for example, in Miller, everybody's bank
15 records in a database that they can search when they had
16 some reasonable articulable suspicion about that
17 everyone. That distinguishes all those prior cases.
18 And I think if you look at the Jones case, you
19 can see the Supreme Court's hesitance to open -- or not
20 hesitance, excuse me, but willingness to possibly
21 reconsider the reasonable expectation of privacy when a
22 third party is involved. You overlay that with the fact
23 that we all know this data is being collected about the
24 citizens outside of any investigation whatsoever; it's
25 simply done to have the data to make it more convenient

1 for the government to search it.
2 The reasonableness argument. I believe that
3 the President's commission on the metadata program
4 provided clear evidence that this can be accomplished
5 other ways. In other words, the phone companies can
6 retain the data just like Smith versus Maryland. If the
7 government has a suspicion, they can go to that phone
8 company, ask for the data, and then investigate it.
9 That would fall squarely within Smith versus Maryland.
10 But I distinguish Smith versus Maryland and
11 all those other cases by the dragnet search and
12 collection of data about every single American. And,
13 frankly, your Honor, that is beyond what the founders of
14 this country intended and the Fourth Amendment when the
15 government has access and saved data about individual
16 citizens for a five-year term and can query it, without
17 that person ever knowing, based on a reasonable
18 articulable suspicion.
19 And, in fact, we never would even have known
20 this program existed unless Mr. Snowden had released
21 those documents in an unlawful manner. But that brings
22 us to where we are today, your Honor, and I think Smith
23 versus Maryland is clearly distinguishable on its face
24 based on the facts and the Court should grant the motion
25 for the preliminary injunction and deny the motion to

1 dismiss.
2 THE COURT: All right. Thank you.
3 Counsel, I appreciate the argument and the
4 quality, both of the argument and the briefing, it
5 really was first class. I'm obviously going to take the
6 matter under advisement, issue a written decision.
7 I was thinking last night as I was reviewing
8 the briefs, I -- this is one of the reasons why I think
9 I have the best job in the world. I get a chance to see
10 really good attorneys arguing about really difficult
11 issues. Sometimes they give me a headache, but that's
12 probably bit of an occupational hazard.
13 We will issue, though, a written decision.
14 We've already started drafting. It's important for me
15 to -- to at least try thinking about the issues in terms
16 of a decision and, you know, I must say, I mean, I have
17 some real sympathy and concerns about how we deal with
18 the Fourth Amendment adopted in 1789 or '91 whenever the
19 Bill of Rights was finally adopted. And most of the --
20 our understanding of that was developed over the last 60
21 or 70 years.
22 But I think most of the critical issues that
23 we're going to have to apply that doctrine to are going
24 to turn upon things that has really happened just in the
25 last 10, 15, 20 years and a world which is changing with

1 just lightening speed. And I don't know how the Court
2 is going to address that. I do think Katz needs to be
3 revisited.
4 We're going to get back to first principles
5 and decide how we apply this notion of an expectation of
6 privacy in a world where one can argue no one has really
7 any expectation of privacy. And if we live in a world
8 of that sort, does the Fourth Amendment become
9 irrelevant or do we figure out a way to redefine it in a
10 way that will have some meaning in this world that we
11 live in.
12 I don't have an answer for that. That's way
13 beyond my pay grade, but it is something that our
14 Supreme Court is going to have to wrestle with and it's
15 one of the reasons I said at the outset that I struggle
16 with any notion that we can use in a (inaudible)
17 philosophy and go back and try to figure out what the
18 drafters of the Bill of Rights meant when they sat in
19 Congress in 1789, what the states were thinking when
20 they ratified it. I just don't think that's a very
21 profitable exercise.
22 I think we have to look the kind of the
23 fundamental underlying values that they were trying to
24 embrace and figure out how those values play out in the
25 21st century. Not an easy task.

In any event, we will take the matter under advisement, issue a written decision in due course. I do, again, appreciate the quality of the argument and the briefing. We'll be in recess.

THE CLERK: All rise.

(End of audio file.)

--oOo--

I, Valerie Nunemacher, certify that the foregoing pages are a true and correct transcription of the audiotaped proceedings to the best of my ability, except where noted "unintelligible" or "inaudible."

Valerie Nunemacher

Valerie Nunemacher, CSR, CCR, RPR

EXHIBIT B

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

ANNA J. SMITH, Plaintiff, v. BARACK OBMAMA, President of the United States, *et al.*, Defendants.	Case No. 2:13-cv-00257-BLW **DECLARATION OF JOHN GIACALONE, ASSISTANT DIRECTOR, COUNTER-TERRORISM DIVISION, FEDERAL BUREAU OF INVESTIGATION**

I, John Giacalone, hereby state and declare as follows:

1. I am the Assistant Director of the Counterterrorism Division, Federal Bureau of Investigation (FBI), United States Department of Justice, a component of an Executive Department of the United States Government. I am responsible for, among other things, directing and overseeing the conduct of investigations originating from the FBI's Counterterrorism Division. As Assistant Director, I have official supervision and control over files and records of the Counterterrorism Division, FBI, Washington, D.C.

2. The FBI submits this declaration in the above-captioned case in support of the Government's opposition to the plaintiff's motion for a preliminary injunction. I base the statements I make in this declaration upon my personal knowledge and information I have obtained in the course of carrying out my duties and responsibilities as Assistant Director.

3. I discuss herein the National Security Agency's (the NSA's) telephony metadata program, authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to Section 215 of the USA PATRIOT Act, under which the NSA obtains and queries bulk telephony metadata for counterterrorism purposes. Although the existence of the program has been publicly acknowledged by the Government, numerous details about its scope and operation remain classified, and cannot be discussed in a public declaration. I therefore limit my discussion herein to facts about the program that are unclassified in nature. I also address in unclassified terms the value of this program as a tool, including as a complement to other classified and unclassified FBI investigatory capabilities not discussed herein, for protecting the United States and its people from terrorist attack. A transition recently ordered by the President to enhance the program's protections for individual privacy while preserving its needed capabilities is discussed in the accompanying declaration submitted by the NSA.

Overview of the NSA Telephony Metadata Program

4. 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. It is imperative that the United States Government have the capability to rapidly identify any terrorist threat inside the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort.

5. One method that the NSA has developed to accomplish this objective is the FISC-authorized bulk collection and analysis of telephony metadata that principally pertains to telephone calls to, from, or within the United States. Under the NSA's telephony metadata program authorized by the FISC, the term "metadata" refers to information that is about telephone calls but does not include cell site location information or the content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Specifically, such telephony metadata include comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. By analyzing telephony metadata based on telephone numbers (or other identifiers) associated with terrorist operatives or activity, NSA analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. The NSA telephony metadata program was specifically developed to assist the Government in detecting communications between known or suspected terrorists who are operating outside of

the United States and who are in contact with others inside the United States, as well as communications between operatives within the United States.

6. Under the NSA telephony metadata program at issue in this case, since May 2006 the FBI has obtained orders from the FISC directing certain telecommunications service providers to produce telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores, queries, and analyzes the metadata for counterterrorism purposes. The FISC issues these orders under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act (Section 215). Under the terms of the FISC's orders, the authority to continue the program must be renewed every 90 days. The FISC first authorized the program in May 2006, and since then it has periodically renewed the program thirty-five (35) times under orders issued by fifteen (15) different FISC judges. As part of a recently announced transition ordered by the President, the Intelligence Community and the Attorney General are to develop options for a new approach that can preserve the program's capability without the Government holding the bulk telephony metadata itself.

7. Under the FISC's orders, the information produced to the NSA is strictly limited to telephony metadata, including the telephone numbers used to make and receive the call, when the call took place, and how long the call lasted. The metadata obtained under this FISC-authorized program do not include any information about the content of those calls. The Government cannot, through this program, listen to or record any telephone conversations. The metadata principally pertain to telephone calls made from foreign countries to the United States, calls made from the United States to foreign countries, and calls within the United States.

8. Telephony metadata can be an important tool in a counterterrorism investigation because analysis of the data permits the Government to determine quickly whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities, including persons and activities within the United States. The NSA Section 215 telephony metadata program is carefully limited to this purpose: it is not lawful for anyone to query the bulk telephony metadata for any purpose other than counterterrorism, and FISC-imposed rules strictly limit all such queries. The program includes a variety of oversight mechanisms to prevent misuse, as well as external reporting requirements to the FISC and the United States Congress.

9. The utility of analyzing telephony metadata as an intelligence tool is not a matter of conjecture. Pen-register and trap-and-trace (PR/TT) devices provide no historical contact information, only a record of contacts with the target occurring after the devices have been installed. For decades reaching back to the Cold-War era, the FBI has relied on contact chaining as a method of detecting foreign espionage networks and operatives, both in the United States and abroad, and disrupting their plans. As discussed below, experience has shown that NSA metadata analysis, in complement with other FBI investigatory and analytical capabilities, produces information pertinent to FBI counterterrorism investigations, and can contribute to the prevention of terrorist attacks. Indeed, in March 2009, the FISC ordered that the continued collection and retention of such metadata be justified by the submission of an affidavit from the Director of the FBI articulating the value of the program. The FBI provided the declaration as ordered and the Court reauthorized the program.

Court Approval

10. Under the Section 215 program at issue, the FBI submits an application to the FISC seeking orders directing named telecommunications service providers to produce to the NSA call detail records created in the ordinary course of business. As required by Section 215, the Government's application contains a statement of facts showing that there are reasonable grounds to believe the records sought are relevant to the FBI's authorized investigations of the specified foreign terrorist organizations. In addition, the application explains that the records are sought for investigations to protect against international terrorism, conducted under guidelines approved by the Attorney General pursuant to Executive Order 12333 (as amended) that concern specified foreign terrorist organizations. The application is supported by a declaration from a senior official of the NSA's Signals Intelligence Directorate (SID).

11. Starting in May 2006, fifteen (15) separate judges of the FISC have granted the Government's applications for bulk production of telephony metadata under this program on thirty-six (36) separate occasions. From time to time, prior to granting the Government's application, the Court convenes a hearing to receive additional evidence and testimony regarding the program and its implementation. On granting an application, the FISC issues a "Primary Order" that recites the court's findings, including that there are reasonable grounds to believe the call detail records sought are relevant to authorized FBI investigations to protect against international terrorism. The Primary Order then provides that certain telecommunications service providers, upon receipt of appropriate Secondary Orders (discussed below), shall produce to the NSA on an ongoing daily basis for the duration of the Primary Order electronic copies of the call detail records created by them containing the "telephony metadata" discussed above,

explicitly excluding the substantive content of any communication, the name, address, or financial information of a subscriber or customer, and cell site location information.

12. The Primary Order also sets a specific date and time on which the NSA's authority to collect bulk telephony metadata from the providers expires, usually within 90 days of the date on which the FISC issues the order, necessitating the submission of an application for additional orders to renew the NSA's authority if the program is to continue.

13. In conjunction with the Primary Order, the FISC also issues a so-called "Secondary Order" to each of the telecommunications service providers identified in the Primary Order. These orders direct the providers, consistent with the Primary Order, to produce "telephony metadata" to the NSA on an ongoing daily basis thereafter for the duration of the Order. Telephony metadata is defined under the Secondary Orders to include (and exclude) the same information as under the Primary Order.

14. These prospective orders for the production of metadata make for efficient administration of the process for all parties involved - the FISC, the Government, and the providers. In theory the FBI could seek a new set of orders on a daily basis for the records created within the preceding 24 hours. But the creation and processing of such requests would impose entirely unnecessary burdens on both the FISC and the FBI - no new information would be anticipated in such a short period of time to alter the basis of the FBI's request or the facts upon which the FISC has based its orders. Providers would also be forced to review daily requests, rather than merely continuing to comply with one ongoing request, a situation that would be more onerous on the providers and raise potential and unnecessary compliance issues. The prospective orders sought and obtained by the FBI merely ensure that the records can be

sought in a reasonable manner for a reasonable period of time (90 days) while avoiding unreasonable and burdensome paperwork.

The NSA's Query and Analysis of the Metadata and Dissemination of the Results

15. Under the FISC orders issued since May 2006, before the NSA may query the metadata acquired under the FISC's orders for intelligence purposes, authorized NSA officials must determine that the identifiers on which the queries will be based are reasonably suspected of being associated with one (or more) of the foreign terrorist organizations specified in the Primary Order. As discussed in the accompanying NSA declaration, at the President's direction the Government is working with the FISC to require the FISC's permission to use proposed identifiers for purposes of querying the database (except in emergency situations) during the transition the President has ordered.

16. The information on which such determinations of "reasonable, articulable suspicion" are based comes from several sources, including the FBI. The FBI, based upon information acquired in the course of one or more counterterrorism investigations, may develop reasons for concluding that a particular identifier, such as a foreign telephone number, is associated with a person (located in the United States or abroad) who is affiliated with one of the specified terrorist organizations. On that basis, the FBI may submit a request to the NSA for further information about that identifier available from the collected telephony metadata.

Investigative Value of Telephony Metadata to the FBI's Counterterrorism Mission

17. Counterterrorism investigations serve important purposes beyond the ambit of routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they

occur. Terrorism investigations also provide the basis for, and inform decisions concerning, other measures needed to protect the national security, including: excluding or removing persons involved in terrorism from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism threats.

18. As a result, national security investigations often have remarkable breadth, spanning long periods of time and multiple geographic regions to identify terrorist groups, their members, and their intended targets, plans, and means of attack, many of which are often unknown to the intelligence community at the outset. National security investigations thus require correspondingly far-reaching means of information-gathering to shed light on suspected terrorist organizations, their size and composition, geographic reach, relation to foreign powers, financial resources, past acts, goals, plans, and capacity for carrying them out, so that their plans may be thwarted before terrorist attacks are launched. Contact chaining information derived from queries and analysis of the Section 215 bulk telephony metadata has contributed to achieving this critical objective.

19. The FBI derives significant value from the advantages of telephony metadata analysis. The FBI is charged with collecting intelligence and conducting investigations to detect, disrupt, and prevent terrorist threats to the national security. The more pertinent information the FBI has regarding such threats, the more likely it will be able to protect against them. The oft-used metaphor is that the FBI is responsible for "connecting the dots" to form a picture of the threats to the national security. Information gleaned from analysis of bulk telephony metadata

provides additional "dots" that the FBI uses to ascertain the nature and extent of domestic threats to the national security.

20. The NSA provides "tips" to the FBI regarding certain telephone numbers resulting from a query of the Section 215 telephony metadata. In certain instances, the FBI has received metadata-based tips containing information not previously known to the FBI about domestic telephone numbers utilized by targets of pending preliminary investigations. The information from the metadata tips has provided articulable factual bases to believe that the subjects posed a threat to the national security such that the preliminary investigations could be converted to full investigations, which, in turn, led the FBI to focus resources on those targets and their activities. The FBI has also re-opened previously closed investigations based upon information contained in metadata tips. In those instances, the FBI had previously exhausted all leads and concluded that no further investigation was warranted. The new information from the metadata tips was significant enough to warrant the re-opening of the investigations.

21. In other situations, the FBI may already have an investigative interest in a particular domestic telephone number prior to receiving a metadata tip from the NSA. Nevertheless, the tip may be valuable if it provides new information regarding the domestic telephone number that re-vitalizes the investigation, or otherwise allows the FBI to focus its resources more efficiently and effectively on individuals who present genuine threats (by helping either to confirm or to rule out particular individuals as subjects for further investigation).

22. Accordingly, the NSA telephony metadata program authorized under Section 215 is a valuable source of intelligence for the FBI that is relevant to FBI-authorized international terrorism investigations.

23. The tips or leads the FBI receives from bulk metadata analysis under this program can also act as an early warning of a possible threat to the national security. The sooner the FBI obtains information about particular threats to the national security, the more likely it will be able to prevent and protect against them. Bulk metadata analysis sometimes provides information earlier than the FBI's other investigative methods and techniques. In those instances, the Section 215 NSA telephony metadata program acts as an "early warning system" of potential threats against the national security. Earlier receipt of this information may advance an investigation and contribute to the FBI preventing a terrorist attack that, absent the metadata tip, the FBI could not.

24. A number of recent episodes illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack. In January 2009, using authorized collection under Section 702 of the Foreign Intelligence Surveillance Act to monitor the communications of an extremist overseas with ties to al-Qa'ida, the NSA discovered a connection with an individual based in Kansas City. The NSA tipped the information to the FBI, which during the course of its investigation discovered that there had been a plot in its early stages to attack the New York Stock Exchange. After further investigation, the NSA queried the telephony metadata to ensure that all potential connections were identified, which assisted the FBI in running down leads. As a result of the investigation, three defendants pled guilty and were convicted of terrorism offenses relating to their efforts to support al-Qa'ida.

25. In October 2009, David Coleman Headley, a Chicago businessman and dual U.S. and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O'Hare airport on a trip to Pakistan. At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack a Danish newspaper that had published cartoons depicting the

Prophet Mohammed. Headley was later charged with support to terrorism based upon his involvement in the planning and reconnaissance for the widely publicized 2008 hotel attack in Mumbai, India. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and put them in context with his U.S.-based planning efforts.

26. In September 2009, using authorized collection under Section 702 to monitor al-Qa'ida terrorists overseas, the NSA discovered that one of the al-Qa'ida-associated terrorists was in contact with an unknown person located in the United States regarding efforts to procure explosive material. The NSA immediately tipped this information to the FBI, which investigated further, and identified the al-Qa'ida contact as Colorado-based extremist Najibullah Zazi. The NSA and the FBI worked together to determine the extent of Zazi's relationship with al-Qa'ida and to identify any other foreign or domestic terrorist links. The NSA received Zazi's telephone number from the FBI and ran it against the Section 215 telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other U.S.-based extremists. Zazi and his co-conspirators were subsequently arrested. Upon indictment, Zazi pled guilty to conspiring to bomb the New York City subway system. In November 2012, Medunjanin was sentenced to life in prison.

Alternatives to the NSA's Bulk Collection of Telephony Metadata

27. The NSA bulk collection program at issue here presents distinct advantages. The contact chaining capabilities offered by the program exceed the chaining that is performed on data collected pursuant to other means, including traditional means of case-by-case intelligence gathering targeted at individual telephone numbers such as subpoena, warrant, national security

letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly defined orders under Section 215. This is so in at least two important respects, namely, the NSA's querying and analysis of the aggregated bulk telephony metadata under this program.

28. First, the agility of querying the metadata collected by the NSA under this program allows for more immediate contact chaining, which is significant in time-sensitive situations of suspects' communications with known or as-yet unknown co-conspirators. For example, if investigators find a new telephone number when an agent of one of the identified international terrorist organizations is captured, and the Government issues a national security letter for the call detail records for that particular number, it would only be able to obtain the first tier of telephone number contacts and, in rare instances, the second tier of contacts if the FBI separately demonstrates the relevance of the second-generation information to the national security investigation. At least with respect to the vast majority of national security letters issued, new national security letters would have to be issued for telephone numbers identified in the first tier, in order to find an additional tier of contacts. The delay inherent in issuing new national security letters would necessarily mean losing valuable time.

29. Second, aggregating the NSA telephony metadata from different telecommunications providers enhances and expedites the ability to identify chains of communications across multiple providers. Furthermore, NSA disseminations provided to the FBI from this program may include the NSA's analysis informed by its unique collection capabilities.

Conclusion

30. As I explained above, the principal objective of FBI counterterrorism investigations is to prevent and protect against potentially catastrophic terrorist attacks on the U.S. homeland and its people before they occur. In each instance, success depends upon detecting and developing a sufficiently clear and complete picture of a terrorist network and its activities in time to thwart its plans. The exploitation of terrorist communications is a critical tool in this effort, and the NSA's analysis of bulk telephony metadata under this FISC-authorized program provides the Government with one means of discovering communications involving unknown terrorist operatives.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 24 day of January, 2014.

JOHN GIACALONE
Assistant Director
Counterterrorism Division
Federal Bureau of Investigation
Washington, D.C.

EXHIBIT 5

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. 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 ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**DECLARATION OF PROFESSOR EDWARD W. FELTEN** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF PROFESSOR EDWARD W. FELTEN

I, Edward W. Felten, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. The plaintiffs in this lawsuit have challenged what they term the "mass call-tracking" program of the National Security Agency, and they have asked me to explain the sensitive nature of metadata, particularly when obtained in the aggregate. Below, I discuss how advances in technology and the proliferation of metadata-producing devices, such as phones, have produced rich metadata trails. Many details of our lives can be gleaned by examining those trails, which often yield information more easily than do the actual content of our communications.

Superimposing our metadata trails onto the trails of everyone within our social group and those of everyone within our contacts' social groups, paints a picture that can be startlingly detailed.

2. I emphasize that I do not in this declaration pass judgment on the use of metadata analysis in the abstract. It can be an extraordinarily valuable tool. But because it can also be an unexpectedly revealing one—especially when turned to the communications of virtually everyone in the country—I write in the hope that courts will appreciate its power and control its use appropriately.

Biography

3. My name is Edward W. Felten. I am Professor of Computer Science and Public Affairs, as well as Director of the Center for Information Technology Policy, at Princeton University.

4. I received a Bachelor of Science degree in Physics from the California Institute of Technology in 1985, a Master's degree in Computer Science and Engineering from the University of Washington in 1991, and a Ph.D. in the same field from the University of Washington in 1993. I was appointed as an Assistant Professor of Computer Science at Princeton University in 1993, and was promoted to Associate Professor in 1999 and to full Professor in 2003. In 2006, I received an additional faculty appointment to Princeton's Woodrow Wilson School of Public and International Affairs.

5. I have served as a consultant or technology advisor in the field of computer science for numerous companies, including Bell Communications Research, International Creative Technologies, Finjan Software, Sun Microsystems, FullComm and Cigital. I have authored numerous books, book chapters, journal articles, symposium articles, and other publications relating to computer science. Among my peer-reviewed publications are papers on the inference

of personal behavior from large data sets[1] and everyday objects,[2] as well as work on the extraction of supposedly protected information from personal devices.[3]

6. I have testified several times before the United States Congress on computer technology issues.

7. In 2011 and 2012, I served as the first Chief Technologist at the U.S. Federal Trade Commission ("FTC"). In that capacity, I served as a senior policy advisor to the FTC Chairman, participated in numerous civil law enforcement investigations, many of which involved privacy issues, and acted as a liaison to the technology community and industry. My privacy-related work at the FTC included participating in the creation of the FTC's major privacy report issued in March 2012,[4] as well as advising agency leadership and staff on rulemaking, law enforcement, negotiation of consent orders, and preparation of testimony.

8. Among my professional honors are memberships in the National Academy of Engineering and the American Academy of Arts and Sciences. I am also a Fellow of the Association of Computing Machinery. A copy of my curriculum vitae is attached as Exhibit 1 to this declaration.

[1] Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten & Vitaly Shmatikov, *"You Might Also Like:" Privacy Risks of Collaborative Filtering*, Proceedings of IEEE Symposium on Security and Privacy (May 2011), http://bit.ly/kUNh4c.

[2] William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman & Edward W. Felten, *Fingerprinting Blank Paper Using Commodity Scanners*, Proceedings of IEEE Symposium on Security and Privacy (May 2009), http://bit.ly/19AoMej.

[3] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum & Edward W. Felten, *Lest We Remember: Cold Boot Attacks on Encryption Keys*, Proceedings of USENIX Security Symposium (August 2008), http://bit.ly/13Ux38w.

[4] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), http://1.usa.gov/HbhCzA.

The Mass Call Tracking Program

9. On June 5, 2013, *The Guardian* disclosed an order issued by the Foreign Intelligence Surveillance Court ("FISC") pursuant to Section 215 of the Patriot Act (the "Verizon Order").[5] This order compelled a Verizon subsidiary, Verizon Business Network Services ("Verizon"), to produce to the National Security Agency ("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."[6] The Director of National Intelligence subsequently acknowledged the authenticity of the Verizon Order.[7]

10. Following the disclosure of the Verizon Order, government officials indicated that the NSA's acquisition of call detail records is not limited to customers or subscribers of Verizon. In particular, the NSA's collection of this data encompasses telephone calls carried by the country's three largest phone companies: Verizon, AT&T, and Sprint.[8] Because these companies provide at least one end of the vast majority of telecommunications connectivity in the country, these

[5] Secondary Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), *available at* http://bit.ly/11FY393.

[6] *Id*. at 2 (emphasis added).

[7] James R. Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc.

[8] *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total.").

statements suggest that the NSA is maintaining a record of the metadata associated with nearly every telephone call originating or terminating in the United States.

11. Assuming that there are approximately 3 billion calls made every day in the United States, and also assuming conservatively that each call record takes approximately 50 bytes to store, the mass call tracking program generates approximately 140 gigabytes of data every day, or about 50 terabytes of data each year.

12. Assuming (again conservatively) that a page of text takes 2 kilobytes of storage, the program generates the equivalent of about 70 million pages of information every day, and about 25 billion pages of information every year.

13. Members of Congress have disclosed that this mass call tracking program has been in place for at least seven years, since 2006.[9]

14. On July 19, 2013, the day that the Verizon Order was set to expire, the Director of National Intelligence disclosed that the FISC had renewed the NSA's authority to collect telephony metadata in bulk.[10]

15. As noted above, the Verizon Order requires the production of "call detail records" or "telephony metadata." According to the order itself, that term encompasses, among other things, the originating and terminating telephone number and the time and duration of any call. Call detail records also typically include information about the location of the parties to the call. *See* 47 C.F.R. § 64.2003 (2012) (defining "call detail information" as "[a]ny information that

[9] *See* Dan Roberts & Spencer Ackerman, *Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006,'* Guardian, June 6, 2013, http://bit.ly/13rfxdu; *id.* (Senator Saxby Chambliss: "This has been going on for seven years."); *see also* ST-09-0002 Working Draft – Office of the Inspector General, National Security Agency & Central Security Service (Mar. 24, 2009), http://bit.ly/14HDGuL.

[10] Press Release, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata, Office of the Director of National Intelligence (July 19, 2013), http://1.usa.gov/12ThYlT.

pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of any call").

16. Although this latter definition of "call detail information" includes data identifying the location where calls are made or received, I will not address mobile phone location information in this declaration. While senior intelligence officials have insisted that they have the legal authority under Section 215 to collect mobile phone location information, they have stated that the NSA is not collecting phone location information "under this program."[11]

17. The information sought from Verizon also includes "session identifying information"—*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc. These are unique numbers that identify the user or device that is making or receiving a call. Although users who want to evade surveillance can make it difficult to connect these numbers to their individual identities, for the vast majority of ordinary users these numbers can be connected to the specific identity of the user and/or device.

18. The information sought from Verizon also includes the "trunk identifier" of telephone calls. This provides information about how a call was routed through the phone network, which naturally reveals information about the location of the parties. For example, even if the government never obtains cell site location information about a call,[12] trunk identifier

[11] *See* Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, Wall St. J., June 16, 2013, http://on.wsj.com/13MnSsp; Pema Levy, *NSA FISA Metadata Surveillance: Is The Government Using Cell Phones To Gather Location Data?*, Int'l Bus. Times, Aug. 2, 2013, http://bit.ly/18WKXOV.

[12] Cell site location information ("CSLI") reflects the cell tower and antenna sector a phone is connected to when communicating with a wireless carrier's network. Most carriers log and retain CSLI for the start and end of each call made or received by a phone, and some carriers log CSLI

information revealing that a domestic call was carried by a cable from Hawaii to the mainland United States will reveal that the caller was in the state of Hawaii at the time the call was placed.

19. In the present case, government officials have stated that the NSA retains telephony metadata gathered under the Verizon Order, and others similar to it, for five years.[13] Although officials have insisted that the orders issued under the telephony metadata program do not compel the production of customers' names, it would be trivial for the government to correlate many telephone numbers with subscriber names using publicly available sources. The government also has available to it a number of legal tools to compel service providers to produce their customer's information, including their names.[14]

Metadata Is Easy to Analyze

20. Telephony metadata is easy to aggregate and analyze. Telephony metadata is, by its nature, *structured data*. Telephone numbers are standardized, and are expressed in a predictable format: In the United States, a three digit area code, followed by a three digit central office exchange code, and then a four digit subscriber number. Likewise, the time and date information

for text messages and data connections as well. Wireless carriers can also obtain CSLI by "pinging" a phone whenever it is turned on, even if it is not engaged in an active call. The precision of CSLI varies according to several factors, and "[f]or a typical user, over time, some of that data will inevitably reveal locational precision approaching that of GPS." *The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. On the Judiciary*, 113th Cong. (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://1.usa.gov/1awvgOa.

[13] *See* Letter from Ronald Weich, Assistant Attorney General, to Hon. Dianne Feinstein & Hon. Saxby Chambliss, Feb. 2, 2011, http://1.usa.gov/1cdFJ1G (enclosing *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization*); Siobhan Gorman & Julian E. Barnes, *Officials: NSA Doesn't Collect Cellphone-Location Records*, Wall St. J., June 16, 2013, http://on.wsj.com/13MnSsp.

[14] *See* 18 U.S.C. § 2709 (national security letter); 18 U.S.C. § 2703(c), (d) (court order for records concerning electronic communication service).

associated with the beginning and end of each call will be stored in a predictable, standardized format.

21. By contrast, the contents of telephone calls are not structured. Some people speak English, others Spanish, French, Mandarin, or Arabic. Some people speak using street slang or in a pidgin dialect, which can be difficult for others to understand. Conversations also lack a common structure: Some people get straight to the point, others engage in lengthy small talk. Speakers have different accents, exhibit verbal stutters and disfluencies. Although automated transcription of speech has advanced, it is still a difficult and error-prone process.

22. In contrast, the structured nature of metadata makes it very easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances over the past 35 years in computing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyze personal communications, including metadata.

23. Innovations in electronic storage today permit us to maintain, cheaply and efficiently, vast amounts of data. The ability to preserve data on this scale is, by itself, an unprecedented development—making possible the maintenance of a digital history that was not previously within the easy reach of any individual, corporation, or government.

24. This newfound data storage capacity has led to new ways of exploiting the digital record. Sophisticated computing tools permit the analysis of large datasets to identify embedded patterns and relationships, including personal details, habits, and behaviors. As a result, individual pieces of data that previously carried less potential to expose private information may now, in the aggregate, reveal sensitive details about our everyday lives—details that we had no intent or expectation of sharing.

25. IBM's Analyst's Notebook and Pen-Link are two such computing tools. Both are widely used by law enforcement and intelligence agencies for this purpose.[15]

26. IBM's Analyst Notebook product is a multi-purpose intelligence analysis tool that includes specific telephony metadata analysis features, which are "routinely" used to analyze large amounts of telephony metadata.[16] IBM even offers training courses entirely focused on using Analyst's Notebook to analyze telephone call records.[17]

27. Pen-Link is a tool that is purpose-built for processing and analyzing surveillance data. It is capable of importing subscriber Call Detail Record ("CDR") data from the proprietary formats

[15] *Public Safety & Law Enforcement Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1avGItq ("IBM® i2® solutions help law enforcers to turn huge volumes of crime data into actionable insights by delivering tools for tactical lead generation, intelligence analysis, crime analysis and predictive analysis."); *see also Defense and National Security Operations*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/18nateN ("IBM i2 solutions for military and national security organizations have been used across the world to process and analyze the vast quantities of information that they collect, to generate actionable intelligence and to share insights that help identify, predict and prevent hostile threats."); *see also* Pen-Link, *Unique Features of Pen-Link v8* at 16 (April 17, 2008), http://bit.ly/153ee9g ("Many U.S. Federal Law Enforcement and Intelligence agencies have acquired agency-wide site license contracts for the use of Pen-Link in their operations throughout the United States…Pen-Link systems are also becoming more frequently used by U.S. intelligence efforts operating in several other countries.").

[16] *Case Studies: Edith Cowan University, IBM i2 Solutions Help University Researchers Catch a Group of Would-Be Hackers*, International Business Machines (Mar. 27, 2013), http://ibm.co/13J2o36 ("Analyzing this volume of data is nothing new to many law enforcement users who routinely analyze tens of thousands of telephone records using IBM® i2® Analyst's Notebook®.").

[17] *Course Description: Telephone Analysis Using i2 Analyst's Notebook*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/1d5QlB8 ("This intermediate hands-on 3-day workshop focuses on the techniques of utilizing i2 Analyst's Notebook to conduct telephone toll analysis…Learn to import volumes of call detail records from various phone carriers, analyze those records and identify clusters and patterns in the data. Using both association and temporal charts, discover how to use different layouts and more advanced tools to analyze telephonic data quickly and effectively.").

used by the major telephone companies,[18] it can import and export call data to several federal surveillance databases,[19] as well as interact with commercial providers of public records databases such as ChoicePoint and LexisNexis. Pen-Link can perform automated "call pattern analysis," which "automatically identifies instances where particular sequences of calls occur, when they occur, how often they occur, and between which numbers and names."[20] As the company notes in its own marketing materials, this feature "would help the analyst determine how many times Joe paged Steve, then Steve called Barbara, then Steve called Joe back."[21]

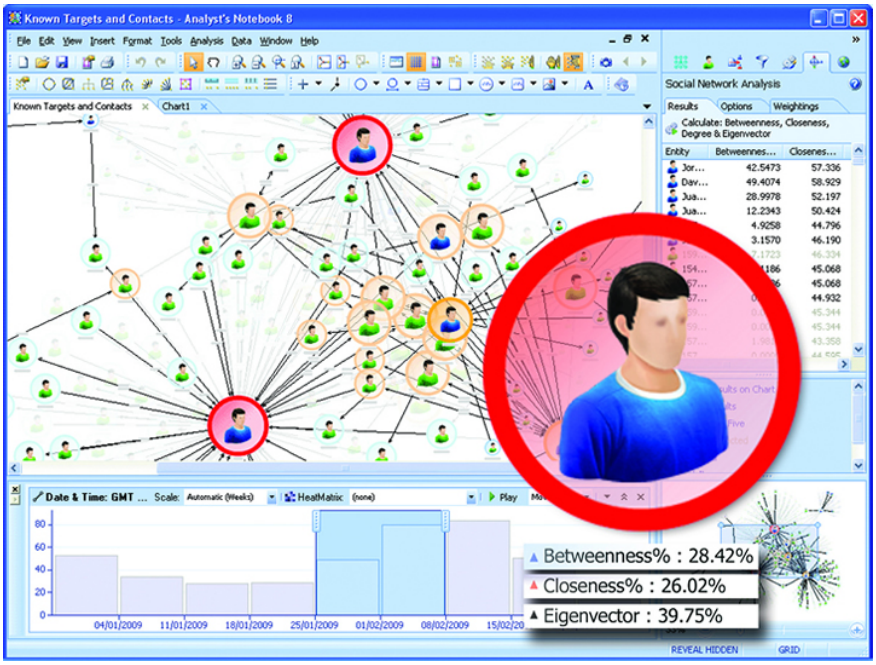

Figure 1: Screenshot of IBM's Analyst Notebook.[22]

[18] *See* Pen-Link, *Unique Features of Pen-Link v8* at 4 (Apr. 17, 2008), http://bit.ly/153ee9g (describing the capability to import 170 different data formats, used by phone companies to provide call detail records).

[19] *Id.* at 4.

[20] *Id.* at 7.

[21] *Id.*

[22] Image taken from *Data Analysis and Visualization for Effective Intelligence Analysis*, International Business Machines (last visited Aug. 22, 2013), http://ibm.co/16qT3hw.

28. The contents of calls are far more difficult to analyze in an automated fashion due to their unstructured nature. The government would first have to transcribe the calls and then determine which parts of the conversation are interesting and relevant. Assuming that a call is transcribed correctly, the government must still try to determine the meaning of the conversation: When a surveillance target is recorded saying "the package will be delivered next week," are they talking about an order they placed from an online retailer, a shipment of drugs being sent through the mail, or a terrorist attack? Parsing and interpreting such information, even when performed manually, is exceptionally difficult. To do so in an automated way, transcribing and data-mining the contents of hundreds of millions of telephone calls per day is an even more difficult task.

29. It is not surprising, then, that intelligence and law enforcement agencies often turn first to metadata. Examining metadata is generally more cost-effective than analyzing content. Of course, the government will likely still have analysts listen to every call made by the highest-value surveillance targets, but the resources available to the government do not permit it to do this for all of the calls of 300 million Americans.

The Creation of Metadata Is Unavoidable

30. As a general matter, it is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats.

31. After decades of research (much of it supported by the U.S. government), there now exist many tools that individuals and organizations can use to protect the confidentiality of their communications content. Smartphone applications are available that let individuals make encrypted telephone calls and send secure text messages.[23] Freely available software can be used

[23] Somini Sengupta, *Digital Tools to Curb Snooping*, N.Y. Times, July 17, 2013, http://nyti.ms/12JKz1s (describing RedPhone and Silent Circle).

to encrypt email messages and instant messages sent between computers, which can frustrate government surveillance efforts traditionally performed by intercepting communications as they are transmitted over the Internet.

32. However, these secure communication technologies protect only the content of the conversation and do not protect the metadata. Government agents that intercept an encrypted email may not know what was said, but they will be able to learn the email address that sent the message and the address that received it as well as the size of the message and when it was sent. Likewise, Internet metadata can reveal the parties making an encrypted audio call and the time and duration of the call, even if the voice contents of the call are beyond the reach of a wiretap.

33. There also exist security technologies specifically designed to hide metadata trails, but those technologies do not work quickly enough to allow real-time communication. The general technique for hiding the origin and destination information for an internet communication involves sending data through a series of intermediaries before it reaches the destination, thus making it more difficult for an entity such as a government agency to learn both the source and destination of the communication. (Such data is conventionally encrypted so that the intermediaries cannot capture it; and a series of intermediaries is used so that no one intermediary knows the identities of both endpoints.)

34. The most popular and well-studied of these metadata hiding systems is The Tor Project, which was originally created by the U.S. Naval Research Lab, and has since received significant funding from the State Department. One significant and widely acknowledged limitation of Tor is the noticeable delay introduced by using the tool. Web browsing conducted through Tor is much slower than through a direct connection to the Internet, as all data must be sent through a series of Tor relays, located in different parts of the world. These volunteer-run relays are

oversubscribed—that is, the demands on the few relays from hundreds of thousands of Tor users are greater than the relays can supply, leading to slowdowns due to "traffic jams" at the relay.

35. Browsing the web using Tor can be painfully slow, in some cases requiring several seconds or longer to load a page. Real-time audio and video communications require a connection with minimal delay, which Tor cannot deliver. Internet telephony and video conferencing services are simply unusable over metadata-protecting systems like Tor.

36. As a result, although individuals can use security technologies to protect the contents of their communications, there exist significant technical barriers that make it difficult, if not impossible, to hide communications metadata, particularly for real-time communications services like Internet telephony and video conferencing.

37. Over the last three decades, and especially with the widespread adoption of mobile phones in the past decade, our reliance on telecommunications has significantly increased. Mobile phones are today ubiquitous, and their use necessarily requires reliance on a service provider to transmit telephone calls, text messages, and other data to and fro. These communications inevitably produce telephony metadata, which is created whenever a person places a call. There is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether.

Telephony Metadata Reveals Content

38. Telephony metadata can be extremely revealing, both at the level of individual calls and, especially, in the aggregate.

39. Although this metadata might, on first impression, seem to be little more than "information concerning the numbers dialed,"[24] analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content.

40. In the simplest example, certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence[25] and rape,[26] including a specific hotline for rape victims in the armed services.[27] Similarly, numerous hotlines exist for people considering suicide,[28] including specific services for first responders,[29] veterans,[30] and gay and lesbian teenagers.[31] Hotlines exist for suffers of various forms of addiction, such as alcohol,[32] drugs, and gambling.[33]

[24] Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act* 15 (Aug. 9, 2013), http://huff.to/1ey9ua5.

[25] *National Domestic Violence Hotline*, The Hotline (last visited Aug. 22, 2013), http://www.thehotline.org.

[26] *National Sexual Assault Hotline*, RAINN: Rape, Abuse & Incest National Network (last visited Aug. 22, 2013), http://www.rainn.org/get-help/national-sexual-assault-hotline.

[27] *About the Telephone Helpline*, DOD Safe Helpline (last visited Aug. 22, 2013), https://www.safehelpline.org/about-safe-helpline.

[28] *District of Columbia/Washington D.C. Suicide & Crisis Hotlines*, National Suicide Hotlines (last visited Aug. 22, 2013), http://www.suicidehotlines.com/distcolum.html.

[29] *Get Help Now! Contact us to Get Confidential Help via Phone or Email*, Safe Call Now (last visited Aug. 22, 2013), http://safecallnow.org.

[30] *About the Veterans Crisis Line*, Veterans Crisis Line (last visited Aug. 22, 2013), http://www.veteranscrisisline.net/About/AboutVeteransCrisisLine.aspx.

[31] *We Provide Crisis Intervention and Suicide Prevention for LGBTQ Youth*, The Trevor Project (last visited Aug. 22, 2013), thttp://www.thetrevorproject.org.

[32] *Alcohol Addiction Helpline*, Alcohol Hotline (last visited Aug. 22, 2013), http://www.alcoholhotline.com.

[33] *What is Problem Gambling*?, National Council on Problem Gambling (last visited Aug. 22, 2013), http://bit.ly/cyosu.

41. Similarly, inspectors general at practically every federal agency—including the NSA[34]—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud.[35] Hotlines have also been established to report hate crimes,[36] arson,[37] illegal firearms[38] and child abuse.[39] In all these cases, the metadata alone conveys a great deal about the content of the call, even without any further information.

42. The phone records indicating that someone called a sexual assault hotline or a tax fraud reporting hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private.

43. In some cases, telephony metadata can reveal information that is even more sensitive than the contents of the communication. In recent years, wireless telephone carriers have partnered with non-profit organizations in order to permit wireless subscribers to donate to charities by sending a text message from their telephones. These systems require the subscriber to send a specific text message to a special number, which will then cause the wireless carrier to add that

[34] Barton Gellman, *NSA Statements to the Post*, Wash. Post, Aug. 15, 2013, http://wapo.st/15LliAB.

[35] *Report Tax Fraud – Tax Fraud Hotline*, North Carolina Department of Revenue (last visited Aug. 22, 2013), http://www.dor.state.nc.us/taxes/reportfraud.html.

[36] *Report Hate Crimes*, LAMBDA GLBT Community Services (last visited Aug. 22, 2013), http://www.lambda.org/hatecr2.htm.

[37] *ATF Hotlines – Arson Hotline*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.

[38] *ATF Hotlines – Report Illegal Firearms Activity*, Bureau of Alcohol, Tobacco, Firearms and Explosives (last visited Aug. 22, 2013), http://www.atf.gov/contact/hotlines/index.html.

[39] *Childhelp National Child Abuse Hotline*, Childhelp (last visited Aug. 22, 2013), http://www.childhelp.org/pages/hotline-home.

donation to the subscriber's monthly telephone bill. For example, by sending the word HAITI to 90999, a wireless subscriber can donate $10 to the American Red Cross.

44. Such text message donation services have proven to be extremely popular. Today, wireless subscribers can use text messages to donate to churches,[40] to support breast cancer research,[41] and to support reproductive services organizations like Planned Parenthood.[42] Similarly, after a policy change in 2012 by the Federal Election Commission, political candidates like Barack Obama and Mitt Romney were able to raise money directly via text message.[43]

45. In all these cases, the most significant information—the recipient of the donation—is captured in the metadata, while the content of the message itself is less important. The metadata alone reveals the fact that the sender was donating money to their church, to Planned Parenthood, or to a particular political campaign.

46. Although it is difficult to summarize the sensitive information that telephony metadata about a single person can reveal, suffice it to say that it can expose an extraordinary amount about our habits and our associations. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations.

[40] *Several Ways to Give*, The Simple Church (2013), http://bit.ly/1508Mgw; *Other Ways to Give*, North Point Church (last visited Aug. 22, 2013), http://bit.ly/16S3IkO.

[41] *Donate by Text*, Susan G. Komen for the Cure (last visited Aug. 22, 2013), http://sgk.mn/19AjGP7.

[42] *Help Support a New Future for Illinois Women and Families*, Planned Parenthood of Illinois (last visited Aug. 22, 2013), http://bit.ly/1bXI2TX.

[43] Dan Eggen, *Text to 'GIVE' to Obama: President's Campaign Launches Cellphone Donation Drive*, Wash. Post, Aug. 23, 2012, http://bit.ly/16ibjCZ.

Aggregated Telephony Metadata Is Even More Revealing

47. When call metadata is aggregated and mined for information across time, it can be an even richer repository of personal and associational details.

48. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a *social graph*. By building a social graph that maps all of an organization's telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the group's membership, donors, political supporters, confidential sources, and so on. Analysis of the metadata belonging to these individual callers, by moving one "hop" further out, could help to classify each one, eventually yielding a detailed breakdown of the organization's associational relationships.

49. For instance, metadata can help identify our closest relationships. Two people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway. More generally, someone you speak to once a year is less likely to be a close friend than someone you talk to once a week.

50. Even our relative power and social status can be determined by calling patterns. As *The Economist* observed in 2010, "People at the top of the office or social pecking order often receive quick callbacks, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organized (sic), such as Friday afternoons."[44]

[44] *Mining Social Networks: Untangling the Social Web*, Economist, Sep. 2, 2010, http://econ.st/9iH1P7.

51. At times, by placing multiple calls in context, metadata analysis can even reveal patterns and sensitive information that would not be discoverable by intercepting the content of an individual communication.

52. Consider the following hypothetical example: A young woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm; followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single telephone call.

53. Likewise, although metadata revealing a single telephone call to a bookie may suggest that a surveillance target is placing a bet, analysis of metadata *over time* could reveal that the target has a gambling problem, particularly if the call records also reveal a number of calls made to payday loan services.

54. With a database of telephony metadata reaching back five years, many of these kinds of patterns will emerge once the collected phone records are subjected to even the most basic analytic techniques.

55. With an organization such as the ACLU, aggregated metadata can reveal sensitive information about the internal workings of the organization and about its external associations and affiliations. The ACLU's metadata trail reflects its relationships with its clients, its legislative contacts, its members, and the prospective whistleblowers who call the organization. Second-order analysis of the telephony metadata of the ACLU's contacts would then reveal even greater details about each of those contacts. For example, if a government employee suddenly begins contacting phone numbers associated with a number of news organizations and then the ACLU and then, perhaps, a criminal defense lawyer, that person's identity as a prospective

whistleblower could be surmised. Or, if the government studied the calling habits of the ACLU's members, it could assemble a detailed profile of the sorts of individuals who support the ACLU's mission.

56. I understand from the plaintiffs that they sometimes represent individuals in so-called "John Doe" lawsuits, where the individuals filing suit request anonymity—and are granted it by the courts—because they are juveniles or because they wish to conceal sensitive medical or psychiatric conditions. In such cases, analysis of aggregated metadata might reveal the anonymous litigant. If, for example, the lawyers in the case have only a handful of contacts in common other than mutual co-workers, and one or more of the lawyers generally call the same one of those common contacts shortly before or after hearings or deadlines in the lawsuit, this would imply the identity of the anonymous litigant. If the attorneys' calling patterns suggest more than one possible identity for the "John Doe," metadata analysis of the candidate individuals could verify the identity of the "John Doe," by correlating facts about the individuals with facts detailed in the lawsuit—for example, that he lives in a particular area (based on the area code of his phone or those of the majority of his contacts), that he has a particular job (based on calls made during work hours), that he has a particular medical condition (based on calls to medical clinics or specialists), or that he holds particular religious or political views (based on telephone donations, calls to political campaigns, or contact with religious organizations).

57. Metadata analysis could even expose litigation strategies of the plaintiffs. Review of the ACLU's telephony metadata might reveal, for example, that lawyers of the organization contacted, for example, an unusually high number of individuals registered as sex offenders in a particular state; or a seemingly random sample of parents of students of color in a racially

segregated school district; or individuals associated with a protest movement in a particular city or region.

58. In short, aggregated telephony metadata allows the government to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant.

Mass Collection of Metadata and Data-Mining Across Many Individuals

59. Advances in the area of "Big Data" over the past few decades have enabled researchers to observe even deeper patterns by mining large pools of metadata that span many telephone subscribers.

60. Researchers have studied databases of call records to analyze the communications reciprocity in relationships,[45] the differences in calling patterns between mobile and landline subscribers,[46] and the social affinity and social groups of callers.[47]

61. Researchers have discovered that individuals have unique calling patterns, regardless of which telephone they are using,[48] they have figured out how to predict the kind of device that is

[45] Lauri Kovanen, Jari Saramaki & Kimmo Kaski, *Reciprocity of Mobile Phone Calls*, Dynamics of Socio-Economic Systems (Feb. 3, 2010), http://arxiv.org/pdf/1002.0763.pdf.

[46] Heath Hohwald, Enrique Frias-Martinez & Nuria Oliver, *User Modeling for Telecommunication Applications: Experiences and Practical Implications* 8, (Data Mining and User Modeling Group, Telefonica Research, 2013), http://bit.ly/1d7WkUU ("Interestingly, Monday is the day with most calls for landline users, while Friday is the day with most calls for mobile users. . . Mobile users spend less time on the phone than landline users.").

[47] Sara Motahari, Ole J. Mengshoel, Phyllis Reuther, Sandeep Appala, Luca Zoia & Jay Shah, *The Impact of Social Affinity on Phone Calling Patterns: Categorizing Social Ties from Call Data Records*, The 6th SNA-KDD Workshop (Aug. 12, 2012), http://b.gatech.edu/1d6i4RY.

making the calls (a telephone or a fax machine),[49] developed algorithms capable of predicting whether the phone line is used by a business or for personal use,[50] identified callers by social group (workers, commuters, and students) based on their calling patterns,[51] and even estimated the personality traits of individual subscribers.[52]

62. The work of these researchers suggests that the power of metadata analysis and its potential impact upon the privacy of individuals increases with the scale of the data collected and analyzed. It is only through access to massive datasets that researchers have been able to identify or infer new and previously private facts about the individuals whose calling records make up the telephone databases. Just as multiple calls by the same person reveal more than a single call, so too does a database containing calling data about millions of people reveal more information about the individuals contained within it than a database with calling data about just one person. As such, a universal database containing records about all Americans' communications will reveal vastly more information, including new observable facts not currently known to the

[48] Corrina Cortes, Daryl Pregibon & Chris Volinsky, *Communities of Interest*, AT&T Shannon Research Labs, http://www.research.att.com/~volinsky/papers/portugal.ps.

[49] Haim Kaplan, Maria Strauss & Mario Szegedy, *Just the Fax – Differentiating Voice and Fax Phone Lines Using Call Billing Data*, AT&T Labs, http://bit.ly/19Aa8Ua.

[50] Corinna Cortes & Daryl Pregibon, *Giga-Mining*, AT&T Labs-Research, http://bit.ly/153pMcI.

[51] Richard A. Becker, Ramon Caceres, Karrie Hanson, Ji Meng Loh, Simon Urbanek, Alexander Varshavsky & Chris Volinsky, *Clustering Anonymized Mobile Call Detail Records to Find Usage Groups*, AT&T Labs-Research, http://soc.att.com/16jmKdz.

[52] Rodrigo de Oliveira, Alexandros Karatzoglou, Pedro Concejero, Ana Armenta & Nuria Oliver, *Towards a Psychographic User Model from Mobile Phone Usage*, CHI 2011 Work-in-Progress (May 7–12, 2011), http://bit.ly/1f51mOy; *see also* Yves-Alexandre de Montjoye, Jordi Quoidbach, Florent Robic & Alex (Sandy) Pentland, *Predicting People Personality Using Novel Mobile Phone-Based Metrics*. Social Computing, Behavioral-Cultural Modeling and Prediction (2013), http://bit.ly/1867vWU.

research community, because no researcher has access to the kind of dataset that the government is presumed to have.

63. A common theme is seen in many of these examples of "big data" analysis of metadata. The analyst uses metadata about many individuals to discover patterns of behavior that are indicative of some attribute of an individual. The analyst can then apply these patterns to the metadata of an individual user, to infer the likely attributes of that user. In this way, the effect of collecting metadata about one individual is magnified when information is collected across the whole population.

64. The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the government to learn information about more people, but it also enables the government to learn new, previously private facts that it could not have learned simply by collecting the information about a few, specific individuals.

Edward W. Felten

Dated: August 23, 2013

EXHIBIT 1

Edward W. Felten

Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University
Sherrerd Hall, Room 302
Princeton NJ 08544
(609) 258-5906
(609) 964-1855 fax
felten@cs.princeton.edu

Education

Ph.D. in Computer Science and Engineering, University of Washington, 1993.
Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.
M.S. in Computer Science and Engineering, University of Washington, 1991.
B.S. in Physics, with Honors, California Institute of Technology, 1985.

Employment

Professor of Computer Science and Public Affairs, Princeton University, 2006-present.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.
Associate Professor of Computer Science, Princeton University, 1999-2003.
Assistant Professor of Computer Science, Princeton University, 1993-99.
Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-present
U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.
U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..
Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.
Certus Ltd.: consultant in product design and analysis, 2000-2002.
Cigital Inc.: Technical Advisory Board member, 2000-2007.

Cloakware Ltd.: Technical Advisory Board member, 2000-2003.
Propel.com: Technical Advisory Board member, 2000-2002.
NetCertainty.com: Technical Advisory Board member, 1999-2002.
FullComm LLC: Scientific Advisory Board member, 1999-2001.
Sun Microsystems: Java Security Advisory Board member, 1997-2001.
Finjan Software: Technical Advisory Board member, 1997-2002.
International Creative Technologies: consultant in product design and analysis, 1997-98.
Bell Communications Research: consultant in computer security research, 1996-97.

Honors and Awards

National Academy of Engineering, 2013.
American Academy of Arts and Sciences, 2011
ACM Fellow, 2007.
EFF Pioneer Award, 2005.
Scientific American Fifty Award, 2003.
Alfred P. Sloan Fellowship, 1997.
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.
NSF National Young Investigator award, 1994.
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.
Best Paper award, 1995 ACM SIGMETRICS Conference.
AT&T Ph.D. Fellowship, 1991-93.
Mercury Seven Foundation Fellowship, 1991-93.

Research Interests

Information security. Privacy. Technology law and policy. Internet software. Intellectual property policy. Using technology to improve government. Operating systems. Interaction of security with programming languages and operating systems. Distributed computing. Parallel computing architecture and software.

Professional Service

Professional Societies and Advisory Groups

ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-present.
DARPA Privacy Panel, 2010-2012.
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.
National Academies study committee on Air Force Information Science and Technology Research, 2004-present.
Electronic Frontier Foundation, Advisory Board, 2004-2007.
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.
DARPA Information Science and Technology (ISAT) study group, 2002-2004.
Co-chair, ISAT study committee on "Reconciling Security with Privacy," 2001-2002.
National Academy study committee on Foundations of Computer Science, 2001-2004.

Program Committees

World Wide Web Conference, 2006.
USENIX General Conference, 2004.
Workshop on Foundations of Computer Security, 2003.
ACM Workshop on Digital Rights Management, 2001.
ACM Conference on Computer and Communications Security, 2001.
ACM Conference on Electronic Commerce, 2001.
Workshop on Security and Privacy in Digital Rights Management, 2001.
Internet Society Symposium on Network and Distributed System Security, 2001.
IEEE Symposium on Security and Privacy, 2000.
USENIX Technical Conference, 2000.
USENIX Windows Systems Conference, 2000.
Internet Society Symposium on Network and Distributed System Security, 2000.
IEEE Symposium on Security and Privacy, 1998.
ACM Conference on Computer and Communications Security, 1998.
USENIX Security Symposium, 1998.
USENIX Technical Conference, 1998.
Symposium on Operating Systems Design and Implementation, 1996.

Boards

Electronic Frontier Foundation, Board of Directors, 2007-2010.
DARPA Information Science and Technology study board, 2001-2003.
Cigital Inc.: Technical Advisory Board.
Sun Microsystems, Java Security Advisory Council.
Cloakware Ltd.: Technical Advisory Board.
Propel.com: Technical Advisory Board.
Finjan Software: Technical Advisory Board.
Netcertainty: Technical Advisory Board.
FullComm LLC: Scientific Advisory Board.

University and Departmental Service

Committee on Online Courses, 2012-present
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
- Member, Executive Committee
- Co-Chair, Interactions with Industry area.
- Co-Chair, Engineering, Policy, and Society area.

Faculty Advisory Committee on Policy, 2002-present.
Council of the Princeton University Community, 2002-present (Executive Committee)
Faculty Advisory Committee on Athletics, 1998-2000.

Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)
Faculty-Student Committee on Discipline, 1996-98.
Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

Students Advised

Ph.D. Advisees:

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy.
Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud.
Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality.
William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.
Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.
J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Assistant Professor of Computer Science, University of Michigan.
Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.
Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Assistant Professor of Computer Science, University of Texas.
Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.
Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.
Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.
Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.
Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Associate Professor of Computer Science, Rice University.

Significant Advisory Role:

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Program Manager at DARPA.
Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Staff technologist at Facedbook.
Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Research Scientist, School of Computer Science, Carnegie Mellon University.

Publications

Books and Book Chapters

[1] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In Open Government, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.

[2] Securing Java: Getting Down to Business with Mobile Code. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.

[3] Java Security: Web Browsers and Beyond. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.

[4] Java Security: Hostile Applets, Holes and Antidotes. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996

[5] Dynamic Tree Searching. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

Journal Articles

[6] Government Data and the Invisible Hand. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. Yale Journal of Law and Technology, vol. 11, 2009.

[7] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Software – Practice and Experience, 33:461-480, 2003.

[8] The Digital Millennium Copyright Act and its Legacy: A View from the Trenches. Illinois Journal of Law, Technology and Policy, Fall 2002.

[9] The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. ACM Transactions on Software Engineering and Methodology, 9:4, October 2000.

[10] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. IEEE Software, 17(5), Sept./Oct. 2000.

[11] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. IEEE Micro 17(1):8-18, February 1997.

[12] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. IEEE Transactions on Parallel and Distributed Computing, February 1997.

[13] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. ACM Transactions on Computer Systems, Nov 1996.

[14] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. IEEE Micro, 15(1):21-28, February 1995.

Selected Symposium Articles

[15] Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2012.

[16] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2011

[17] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.

[18] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.

[19] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.

[20] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17th Network and Distributed System Security Symposium, 2010.

[21] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham, Proc. Electronic Voting Technology Workshop, 2009.

[22] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.

[23] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.

[24] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.

[25] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.

[26] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.

[27] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[28] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.

[29] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

[30] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14th World Wide Web Conference, 2005.

[31] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.

[32] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3rd Workshop on Privacy in Electronic Society. November 2004.

[33] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.

[34] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.

[35] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11th USENIX Security Symposium, August 2002.

[36] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)

[37] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.

[38] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.

[39] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.

[40] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.

[41] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.

[42] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.

[43] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

[44] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.

[45] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.

[46] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20th National Information Systems Security Conference, Oct. 1997.

[47] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.

[48] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)

[49] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.

[50] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.

[51] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.

[52] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.

[53] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.

[54] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[55] Improving Release-Consistent Shared Virtual Memory using Automatic Update . Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996

[56] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

[57] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.

[58] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.

[59] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.

[60] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.

[61] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.

[62] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.

[63] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.

[64] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

Selected Other Publications

[65] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. American Scientist, 97:4. July/August 2009.

[66] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.

[67] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.

[68] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy,* Jan./Feb. 2006.

[69] Inside RISKS: DRM and Public Policy. Edward W. Felten. Communications of the ACM, 48:7, July 2005.

[70] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. IEEE Security and Privacy, May 2003.

[71] A Skeptical View of DRM and Fair Use. Edward W. Felten. Communications of the ACM 46(4):56-61, April 2003.

[72] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.

[73] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.

[74] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.

[75] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.

[76] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.

[77] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.

[78] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.

[79] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.

[80] Inside RISKS: Webware Security. Edward W. Felten. Communications of the ACM, 40(4):130, 1997.

[81] Simplifying Distributed File Systems Using a Shared Logical Disk.Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

[82] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.

[83] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.

[84] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.

[85] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.

[86] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.

[87] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.

[88] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.

EXHIBIT 1

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE
FEDERAL BUREAU OF INVESTIGATION
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.

Docket Number: BR

13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (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 (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

Derived from: Pleadings in the above-captioned docket
Declassify on: 12 April 2038

on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: 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. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- *Remainder of page intentionally left blank.* --

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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 DECLARATION OF ANNA J. SMITH IN SUPPORT OF PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION

I, ANNA J. SMITH, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. I am the Plaintiff in this case.

2. I am a Verizon Wireless customer and I have been for at least 3 years.

3. I use my cell phone to make phone calls almost exclusively.

4. I do have a home phone, but in the past 12 months I have probably made 3 calls on it.

5. I use my cell phone to call my doctor, pastor, my daughters' teachers, my lawyers, and everyone else.

6. I expect that who I call is not shared with the government.

7. I expect that when I call someone is not shared with the government.

8. I expect the length of my calls is not shared with the government.

9. When I learned that information related to my cell phone calls was being shared with the government, I felt this was a violation of my privacy rights.

10. I consider the information that is being provided to the government by Verizon Wireless to be private and I expect Verizon Wireless to keep it private.

I declare under penalty of perjury under the laws of the state of Idaho, that to the best of my knowledge and belief, that the foregoing is true and correct.

DATED this 20th day of December, 2013.

A. Smith

ANNA J. SMITH

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 AMENDED COMPLAINT

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. Plaintiff Anna Smith ("Anna") challenges the government's gathering of her telephone records and location information under Section 215 of the Patriot Act, 50 U.S.C. § 1861.[1]

JURISDICTION AND VENUE

2. Article III of the Constitution and 28 U.S.C. § 1331 provides jurisdiction to this Court because this case arises under the Constitution and the laws of the United States and presents a federal question.

3. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201-2202.

4. The Court has authority to award costs and attorneys fees under 28 U.S.C. § 2412.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (c)(2).

PLAINTIFF

6. Anna is a neonatal intensive care nurse and a mother of two daughters.

7. Anna is a current Verizon Wireless subscriber and a resident of Kootenai County, Idaho.

8. Anna has been a customer of Verizon for at least 3 years and previously was a customer of AT&T Wireless for 4 years.

DEFENDANTS

9. Defendant Barack H. Obama is the President of the United States. President Obama has ultimate authority over executive branch of the government.

[1] "The Patriot Act" is formally referred to as Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

10. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). Defendant Clapper has authority over the activities of the intelligence community.

11. Defendant Lt. Gen. Keith B. Alexander is the Director of the National Security Agency ("NSA") and the Chief of the Central Security Service. Defendant Lt. Gen. Alexander has authority for supervising and implementing all operations and functions of the National Security Agency ("NSA"), the agency responsible for conducting surveillance authorized by the challenged law.

12. Defendant Charles T. Hagel is the Secretary of Defense. Defendant Hagel has authority over the Department of Defense, of which the NSA is a component.

13. Defendant Eric H. Holder is the Attorney General of the United States. Attorney General Holder has authority over the Department of Justice and the Federal Bureau of Investigation ("FBI") and is responsible for overseeing aspects of the challenged statute.

14. Defendant James B. Comey is the Director of the FBI and is responsible for applications made to the Foreign Intelligence Surveillance Court ("FISC") under Section 215 of the Patriot Act.

PLAINTIFF'S ALLEGATIONS

15. It is now commonly known and acknowledged that the Verizon Business Network Services, Inc. is ordered by FISC to provide metadata for each subscriber on its network on a daily basis to the government.

16. Upon information and belief, Anna believes a similar order was issued to Verizon Wireless, which is a joint venture between Verizon Communications, Inc. and Vodafone (hereinafter referred to as "Verizon Wireless").

17. Even if Verizon Wireless was not ordered to produce the metadata by the FISC, the government still captures Anna's personal information because "nearly all calls eventually travel over networks owned by U.S. companies that work with the NSA." This captures 99% of all phone traffic in the United States. Wall Street Journal, June 14, 2013 available at http://online.wsj.com/news/articles/SB10001424127887324049504578543800240266368 last accessed November 4, 2013.

18. As with many Americans, Anna's primary means of communication is with her cell phone.

19. Anna communicates with her family, friends, employer, her children's teachers, her doctor, her legal counsel, and nearly every one else with her cell phone.

20. None of these communications relate in anyway to international terrorism or clandestine intelligence activities.

21. Anna has a subjective expectation of privacy that metadata from these communications is not collected, stored and monitored by the government.

22. The collection of metadata constitutes a violation of a legitimate expectation of privacy and, as an American citizen, Anna asserts that she has a reasonable expectation of privacy that metadata of her calls is not being gathered, stored and monitored by the government.

23. Though Anna voluntarily provides this information to a third-party (Verizon Wireless), she reasonably expects that this information will not shared with the government without her knowledge and consent or, at least, without a showing of probable cause.

24. This monitoring is distressing and a violation of Anna's Constitutional rights.

CAUSES OF ACTION

25. The Mass Call Tracking exceeds the authority granted by 50 U.S.C. § 1861, and thereby violates 5 U.S.C. § 706.

26. The Mass Call Tracking violates the First Amendment to the Constitution.

27. The Mass Call Tracking violates the Fourth Amendment to the Constitution.

PRAYER FOR RELIEF

WHEREFORE the plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over this Complaint;

2. Declare that the Mass Call Tracking violates 50 U.S.C. § 1861 and 5 U.S.C. § 706;

3. Declare that the Mass Call Tracking violates the First and Fourth Amendments of the Constitution;

4. Permanently enjoin Defendants from continuing to gather metadata on Plaintiff Anna Smith;

5. Order Defendants to purge all of metadata of Plaintiff Anna Smith's communications collected pursuant to the Mass Call Tracking;

6. Award Plaintiff Anna Smith fees and costs pursuant to 28 U.S.C. § 2412;

7. Grant such other and further relief as the Court deems just and proper.

DATED this 4th day of November, 2013.

LUKINS & ANNIS, P.S.

By _____
PETER J. SMITH IV, ISB 6997
Co-Counsel for Plaintiff
ANNA J. SMITH

APPEAL,LC1,TERMED

U.S. District Court
District of Idaho (LIVE Database)Version 5.1.1 (CDA - Northern)
CIVIL DOCKET FOR CASE #: 2:13-cv-00257-BLW

Smith v. Obama et al
Assigned to: Judge B. Lynn Winmill
Case in other court: Ninth Circuit Court of Appeals, 14-35555
Cause: 28:1331 Fed. Question

Date Filed: 06/12/2013
Date Terminated: 06/03/2014
Jury Demand: None
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: U.S. Government Defendant

Plaintiff

Anna Jo Smith
a Married Woman

represented by **Lucas Todd Malek**
Luke Malek, Attorney at Law, PLLC
721 N. 8th Street
Couer d'Alene, ID 83814
208-661-3881
Email: luke_malek@hotmail.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Peter J Smith , IV
Lukins & Annis, P.S.
601 E. Front Avenue, Suite 502
Coeur d'Alene, Id 83814
208.667.0517
Fax: 208.664.4125
Email: pjs@lukins.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Barack H. Obama
in his official capacity as President of the United States of America

represented by **Bryan Dearinger**
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., Room 7334
Washington, DC 20001
(202) 514-3489

Fax: (202) 616-8470
Email: bryan.dearinger@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
United States Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
202-514-3358
Email: james.gilligan@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave. , N.W., Room 7132
Washington, DC 20001
(202) 514-2205
Fax: (202) 616-8470
Email: marcia.berman@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
U.S. Department of Justice
20 Massachusetts Ave. N.W.
Washington, DC 20001
202-305-7919
Email: rodney.patton@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
U.S. Attorney's Office
800 E. Park Blvd., Suite 600 Plaza 4
Boise, ID 83712
208 334 9122
Email: Syrena.Hargrove@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

James R. Clapper
in his official capacity as Director of National Intelligence

represented by **Bryan Dearinger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Keith B. Alexander
in his official capacity as Director of the National Security Agency and Chief of the Central Security Service

represented by **Bryan Dearinger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Charles T. Hagel
in his official capacity as Secretary of Defense

represented by **Bryan Dearinger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

Eric H. Holder
in his official capacity as Attorney General of the United States

represented by **Bryan Dearinger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

James B. Comey
in his official capacity as Director of the Federal Bureau of Investigation

represented by **Bryan Dearinger**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

James Jordan Gilligan
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Marcia Berman
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Rodney Patton
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Syrena Case Hargrove
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text

07/14/2014	33 R	ORDER of USCA as to 29 R Notice of Appeal filed by Anna Jo Smith (jp) (Entered: 07/15/2014)
07/01/2014	32 R	USCA Scheduling Order as to 29 R Notice of Appeal filed by Anna Jo Smith. (Notice sent by e-mail to Court Reporter) (cjm)
07/01/2014	31 R	USCA Case Number 14-35555 for 29 R Notice of Appeal filed by Anna Jo Smith. (cjm)
07/01/2014	30 R	TRANSCRIPT REQUEST by Anna Jo Smith for proceedings held on 5/15/2014 before Judge Winmill, re 29 R Notice of Appeal (Notice sent by e-mail to Court Reporter) Transcript due by 9/2/2014. (Smith, Peter)
07/01/2014	29 R	NOTICE OF APPEAL as to 28 R Judgment, by Anna Jo Smith. Filing fee $ 505, receipt number 0976-1177889. (Notice sent to Court Reporter & 9th Cir) (Smith, Peter)(14-35555)
06/03/2014	28 R	JUDGMENT. In accordance with the Memorandum Decision filed with this Judgment, NOW THEREFORE IT IS HEREBY ORDERED, ADJUDGED, AND DECREED, that the motion for injunction 8 is DENIED. IT IS FURTHER ORDERED, ADJUDGED, AND DECREED, that the motion to dismiss 14 R is GRANTED, and the Clerk is directed to close this case. Signed by Judge B. Lynn Winmill. (caused to be mailed to non Registered Participants at the addresses listed on the Notice of Electronic Filing (NEF) by (st)
06/03/2014	27 R	MEMORANDUM DECISION. The Court will grant the defendants' motion to dismiss and deny Smith's motion for injunctive relief. The Court will issue a separate Judgment as required by Rule 58(a). Signed by Judge B. Lynn Winmill. (caused to be mailed to non Registered Participants at the addresses listed on the Notice of Electronic Filing (NEF) by (st)
05/15/2014	26 R	Minute Entry for proceedings held before Judge B. Lynn Winmill: Motion Hearing held on 5/15/2014 re 14 R MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM MOTION to Dismiss for Lack of Jurisdiction filed by James B. Comey, Keith B. Alexander, Charles T. Hagel, James R. Clapper, Barack H. Obama, Eric H. Holder, 8 MOTION for Preliminary Injunction filed by Anna Jo Smith. MOTIONS TAKEN UNDER ADVISEMENT. (Court Reporter/ESR Annie Williams.) (lp)
05/05/2014	25	NOTICE by Keith B. Alexander, James R. Clapper, James B. Comey, Eric H. Holder, Barack H. Obama *of Recent Authority* (Attachments: # 1 Exhibit (March 20, 2014 FISC Opinion & Order))(Gilligan, James)
04/14/2014		Reset Hearing as to 14 R Motion to Dismiss and 8 Motion for Preliminary Injunction pursuant to Order 24 . Motion Hearing reset for 5/15/2014 at 9:00 AM in Coeur d Alene - District Courtroom before Judge B. Lynn Winmill. (jlg)

04/10/2014	24	DOCKET ENTRY ORDER granting 23 R Joint Motion to Vacate Hearing Date. The new hearing date shall be May 15, 2014, at 9:00 a.m. in the Federal Courthouse in Coeur d'Alene, Idaho. Signed by Judge B. Lynn Winmill. (caused to be mailed to non Registered Participants at the addresses listed on the Notice of Electronic Filing (NEF) by (dm)
04/04/2014	23 R	Joint MOTION To Reschedule and Relocate Motions Hearing James Jordan Gilligan appearing for Defendants Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Barack H. Obama, Plaintiff Anna Jo Smith. Responses due by 4/28/2014 (Gilligan, James)
04/02/2014	22	DOCKET ENTRY NOTICE OF HEARING ON MOTIONS - The Court will hear oral argument regarding the following motions on 4/16/2014 at 2:00 PM in Boise - Courtroom 3 before Judge B. Lynn Winmill: 8 Motion for Preliminary Injunction and 14 R Motion to Dismiss. (jlg)
04/01/2014		The 60 day deadline has expired. Case will remain with District Judge. No more notice of availability or assignment will be sent out. Consent deadline(s) termed. (jp)
03/14/2014	21 R	REPLY to Response to Motion re 14 R MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM MOTION to Dismiss for Lack of Jurisdiction filed by Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III, Barack H. Obama. (Gilligan, James)
03/08/2014	20	NOTICE by Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III, Barack H. Obama *(Defendants Corrected Notice Regarding Order of the Foreign Intelligence Surveillance Court)* (Attachments: # 1 Exhibit, # 2 Exhibit)(Gilligan, James)
03/07/2014	19 R	NOTICE by Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III, Barack H. Obama *(Notice Regarding Order of the Foreign Intelligence Surveillance Court)* (Gilligan, James)
03/03/2014	18 R	RETURN MAIL undelivered as to Rodney Patton re: 16 R Notice of Availability Setting Deadline filed by Anna Jo Smith, James B. Comey, Keith B. Alexander, Charles T. Hagel, James R. Clapper, Barack H. Obama, Eric H. Holder. (st)
02/21/2014	17 R	MEMORANDUM in Opposition re 14 R MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM MOTION to Dismiss for Lack of Jurisdiction , 8 MOTION for Preliminary Injunction *Reply Brief* filed by Anna Jo Smith. Replies due by 3/10/2014.(Smith, Peter)
01/27/2014	16 R	NOTICE of Availability of Magistrate Judge and Requirement for Consent sent to counsel for Plaintiff & Defendants. Consent/Objection to Magistrate due by 3/31/2014. (jp)

01/24/2014		Set/Reset Deadlines as to 14 R MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM MOTION to Dismiss for Lack of Jurisdiction . Per Order dkt 12, Responses due by 2/21/2014 Replies due by 3/14/2014. (jp) (Entered: 01/27/2014)
01/24/2014	15 R	MEMORANDUM in Opposition re 8 MOTION for Preliminary Injunction filed by Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III, Barack H. Obama. Replies due by 2/10/2014. (Attachments: # 1 Affidavit (Declaration of James J. Gilligan), # 2 Exhibit A, # 3 Exhibit B, # 4 Exhibit C, # 5 Exhibit D, # 6 Exhibit E, # 7 Exhibit F, # 8 Exhibit G, # 9 Exhibit H, # 10 Exhibit I, # 11 Exhibit J, # 12 Exhibit K, # 13 Exhibit L, # 14 Exhibit M, # 15 Exhibit N, # 16 Exhibit O, # 17 Exhibit P, # 18 Exhibit Q, # 19 Exhibit R)(Gilligan, James) Modified on 2/21/2014 to link to dkt 14 R (jp).
01/24/2014	14 R	MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM , MOTION to Dismiss for Lack of Jurisdiction (Responses due by 2/18/2014)James Jordan Gilligan appearing for Defendants Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Barack H. Obama. (Attachments: # 1 R Memorandum in Support (Memorandum in Support of Defendants' Motion to Dismiss and in Opposition to Plaintiff's Motion for a Preliminary Injunction))(Gilligan, James)
01/17/2014	13	DOCKET ENTRY NOTICE OF HEARING regarding 8 Motion for Preliminary Injunction: A Motion Hearing is set for 4/16/2014 at 2:00 PM in Boise - Courtroom 3 before Judge B. Lynn Winmill. (jlg)
01/15/2014		Set/Reset Deadlines as to 8 MOTION for Preliminary Injunction . Per dkt 12 Responses due by 1/24/2014 Replies due by 2/21/2014. (jp) (Entered: 01/16/2014)
01/15/2014	12 R	SCHEDULING ORDER granting 10 R Joint Motion for a Briefing Schedule and Enlargement of Page Limitations. Up to 45 pages for Defendants' Combined Brief in Opposition to Plaintiff's Motion for a Preliminary Injunction and in Support of Defendants' Motion to Dismiss, to be filed not later than 1/24/14; Up to 45 pages for Plaintiff's Combined Reply in Support of Plaintiff's Motion for a Preliminary Injunction and Opposition to Defendants' Motion to Dismiss, to be filed not later than 2/21/14014; and Up to 25 pages for Defendants' Reply Brief in Support of Defendants' Motion to Dismiss, to be filed not later than 3/14/14. Signed by Judge B. Lynn Winmill. (caused to be mailed to non Registered Participants at the addresses listed on the Notice of Electronic Filing (NEF) by (jp) (Entered: 01/16/2014)
01/07/2014	10 R	Joint MOTION for entry of briefing schedule and enlargement of page limits re 3 R Amended Complaint, 8 MOTION for Preliminary Injunction James Jordan Gilligan appearing for Defendants Keith B. Alexander, James R.

		Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Barack H. Obama, Plaintiff Anna Jo Smith. Responses due by 1/31/2014 (Gilligan, James)
01/02/2014	11 R	RETURN MAIL undelivered as to Rodney Patton re: 7 R Notice of Assignment (jp) (Entered: 01/07/2014)
12/23/2013		DOCKET ENTRY NOTICE of Case Number Change, Case reassigned to Judge B. Lynn Winmill for all further proceedings. Judge Ronald E. Bush no longer assigned to case. Please use this case number on all future pleadings, 2:13-cv-257-BLW (jp)
12/23/2013	9 R	ORDER OF REASSIGNMENT the Clerk of the Court shall reassign this matter to a United States District Judge for all further proceedings. Signed by Judge Ronald E. Bush. (caused to be mailed to non Registered Participants at the addresses listed on the Notice of Electronic Filing (NEF) by (jp)
12/20/2013	8	MOTION for Preliminary Injunction Peter J Smith, IV appearing for Plaintiff Anna Jo Smith. Responses due by 1/13/2014 (Attachments: # 1 R Memorandum in Support of Motion for a Preliminary Injunction, # 2 R Affidavit of Anna J. Smith in Support of Motion for a Preliminary Injunction, # 3 R Affidavit of Peter J. Smith in Support of Motion for a Preliminary Injunction, # 4 R Exhibit 1 of Affidavit of Peter J. Smith IV, # 5 R Exhibit 2 of Affidavit of Peter J. Smith IV, # 6 R Exhibit 3 of Affidavit of Peter J. Smith IV, # 7 R Exhibit 4 of Affidavit of Peter J. Smith IV, # 8 R Exhibit 5 of Affidavit of Peter J. Smith IV)(Smith, Peter)
12/03/2013	7 R	NOTICE of Assignment to Magistrate Judge and Requirement for Consent sent to counsel for Keith B. Alexander, James R. Clapper, James B. Comey, Charles T. Hagel, Eric H. Holder, Barack H. Obama, Anna Jo Smith re 1 R Complaint, 6 R Notice of Appearance. Consent/Objection to Magistrate due by 2/6/2014. (jp)
12/02/2013	6 R	NOTICE of Appearance by James Jordan Gilligan on behalf of All Defendants (Gilligan, James)
11/08/2013	5 R	Summons Issued as to James B. Comey, (Print attached Summons for service.) (jp)
11/07/2013	4	Civil Cover Sheet re 3 R Amended Complaint filed by Anna Jo Smith. (Attachments: # 1 Summons Def Comey Summons)(Smith, Peter)
11/07/2013	3 R	AMENDED COMPLAINT against Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Barack H. Obama, James B. Comey, filed by All Plaintiffs.(Smith, Peter)
06/17/2013	2	Summons Issued as to All Defendants (Print attached Summons for service.) (Attachments: # 1 Summons 2, # 2 Summons 3, # 3 Summons 4, # 4 Summons 5, # 5 Summons 6)(krb)

06/12/2013	1 R	COMPLAINT against All Defendants (Filing fee $ 400 receipt number 0976-1027809.), filed by All Plaintiffs. (Attachments: # 1 R Cover Sheet, # 2 R Summons All Summonses Combined)(Smith, Peter)

PACER Service Center			
Transaction Receipt			
08/22/2014 15:09:52			
PACER Login:	ef0084:2543583:0	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	2:13-cv-00257-BLW
Billable Pages:	8	**Cost:**	0.80