

1 CINDY COHN (SBN 145997)
cindy@eff.org
2 LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
3 JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
4 ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
5 San Francisco, CA 94109
Telephone: (415) 436-9333
6 Fax: (415) 436-9993

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111-1704
Telephone: (415) 391-5400
Fax: (415) 397-7188

7 RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
8 LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
9 San Francisco, CA 94111
Telephone: (415) 433-3200
10 Fax: (415) 433-6382

THOMAS E. MOORE III (SBN 115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Fax: (650) 798-5001

11 ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
12 LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
13 Berkeley, CA 94703
Telephone: (510) 289-1626

14 Attorneys for Plaintiffs

15
16
17 UNITED STATES DISTRICT COURT
18 FOR THE NORTHERN DISTRICT OF CALIFORNIA

19)
20) CAROLYN JEWEL, TASH HEPTING,
21) YOUNG BOON HICKS, as executrix of the
22) estate of GREGORY HICKS, ERIK KNUTZEN
23) and JOICE WALTON, on behalf of themselves
24) and all others similarly situated,
25)
26) Plaintiffs,
27)
28)
29) v.
30)
31) NATIONAL SECURITY AGENCY, *et al.*,
32)
33) Defendants.
34)

CASE NO. 08-CV-4373-JSW

DECLARATION OF THOMAS E. MOORE III IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' STAY REQUEST

Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

1 I, Thomas E. Moore III, do hereby declare:

2 1. I am a member in good standing of the Bar of the State of California and the bar of
3 this Court. I am counsel to plaintiffs in this action. Plaintiffs submit the following evidence for the
4 Court's consideration. I certify that each exhibit attached hereto is a true and correct copy of the
5 document located at the indicated source.

6 2. Attached hereto as **Exhibit A** is the April 25, 2013 Secondary Order of the Foreign
7 Intelligence Surveillance Court (the "FISC Order"), authorizing the collection of all call data
8 records and communications metadata from communications transiting the network of a Verizon
9 operating subsidiary known as Verizon Business Network Services, Inc. This order was obtained
10 from the website of the *Guardian* newspaper, which published it June 6, 2013:

11 <http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order>.

12 3. Attached hereto as **Exhibit B** is a June 6, 2013 statement by Director of National
13 Intelligence James Clapper confirming the authenticity of the FISC Order published by the
14 *Guardian*. DNI Clapper described the FISC Order as a "U.S. court document" and said "[t]he
15 judicial order that was disclosed in the press is used to support a sensitive intelligence collection
16 operation" He further stated: "The collection . . . is broad in scope" and "The FISA Court
17 specifically approved this method of collection" Available at:

18 [http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information)
19 [statement-on-recent-unauthorized-disclosures-of-classified-information](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information).

20 When asked in a subsequent interview, "Why do you need every telephone number? Why
21 is it such a broad vacuum cleaner approach?" DNI Clapper responded, "Well, you have to start
22 someplace." June 8, 2013 NBC News interview, attached hereto as **Exhibit C**. Available at:

23 [http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-](http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell)
24 [2013/874-director-james-r-clapper-interview-with-andrea-mitchell](http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell).

25 4. In response to disclosure of the FISC Order, several members of Congress have
26 made statements confirming the ongoing untargeted dragnet acquisition of communications
27 records. Attached hereto as **Exhibit D** is a transcript published by the *Washington Post* of a joint
28 press conference on June 6, 2013 by Senator Dianne Feinstein and Senator Saxby Chambliss,

1 respectively the Chairman and the Vice Chairman of the Senate Select Committee on Intelligence,
2 confirming the existence of the communications records collection program and stating that it has
3 been going on pursuant to FISC orders for seven years. Senator Feinstein: “As far as I know, this
4 is the exact three month renewal of what has been the case for the past seven years.” Senator
5 Chambliss: “Let me just emphasize, this is nothing particularly new. This has been going on for
6 seven years under the auspices of the FISA authority and every member of the United States Senate
7 has been advised of this.” (Available at: [http://www.washingtonpost.com/blogs/post-](http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/?print=1)
8 [politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-](http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/?print=1)
9 [records-program/?print=1](http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/?print=1).)

10 Attached hereto as **Exhibit E** is a report published by CBS News of Senate Majority Leader
11 Harry Reid’s June 6, 2013 statement regarding the disclosure of the FISC Order, in which he said:
12 “Right now I think everyone should just calm down and understand that this isn’t anything that is
13 brand new, it’s been going on for some seven years” Video available at:
14 [http://www.cbsnews.com/8301-250_162-57588058/nsas-verizon-records-collection-calm-down-](http://www.cbsnews.com/8301-250_162-57588058/nsas-verizon-records-collection-calm-down-reid-says/)
15 [reid-says/](http://www.cbsnews.com/8301-250_162-57588058/nsas-verizon-records-collection-calm-down-reid-says/).

16 5. Attached hereto as **Exhibit F** is a news story published June 7, 2013 by the *Wall*
17 *Street Journal* confirming that AT&T and Sprint are subject to dragnet communications records
18 collection orders similar to the Verizon order. Available at:
19 <http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html>.

20 6. Attached hereto as **Exhibit G** is a June 6, 2013 letter to Attorney General Eric
21 Holder from House Judiciary Committee Chairman Rep. James Sensenbrenner, co-author of the
22 Patriot Act amendments to FISA which the FISC Order rests upon. Rep. Sensenbrenner stated: “I
23 do not believe the released FISA order is consistent with the requirements of the Patriot Act. How
24 could the phone records of so many innocent Americans be relevant to an authorized investigation
25 as required by the Act?” Available at:
26 [http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holde](http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf)
27 [r.pdf](http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf).

1 In a separate statement the same day, Rep. Sensenbrenner said: “Seizing phone records of
2 millions of innocent people is excessive and un-American.” Available at:

3 <http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337001>.

4 Attached hereto as **Exhibit H** is an op-ed that Rep. Sensenbrenner wrote that was published
5 in the *Guardian* June 9, 2013 describing the history of the Patriot Act and explaining further why
6 the communications records program is unlawful. He states: “[B]ased on the scope of the released
7 order, both the administration and the Fisa court are relying on an unbounded interpretation of the
8 [Patriot] act that Congress never intended. [¶] The released Fisa order requires daily productions of
9 the details of every call that every American makes, as well as calls made by foreigners to or from
10 the United States. . . . [¶] This is well beyond what the Patriot Act allows.” Available at:

11 <http://www.guardian.co.uk/commentisfree/2013/jun/09/abuse-patriot-act-must-end/print>.

12 Also available at:

13 <http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337542>.

14 7. President Barak Obama has also confirmed the existence of the untargeted
15 communications records collection dragnet. Attached hereto as **Exhibit I** is a transcript published
16 by the *Wall Street Journal* of the President’s remarks at a June 7, 2013 press conference regarding
17 the government’s electronic surveillance operations. In it, he confirmed that “what the intelligence
18 community is doing is looking at phone numbers and durations of calls;” “this so-called metadata.”
19 He gave as an example the government’s possession of the communications records of *New York*
20 *Times* White House correspondent Jackie Calmes. Available at:

21 [http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-](http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/tab/print/)
22 [controversy/tab/print/](http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/tab/print/).

23 8. Attached hereto as **Exhibit J** is the transcript of a June 9, 2013 National Public
24 Radio *Weekend Edition* interview with General Michael Hayden (retired), former NSA Director
25 and former CIA Director and one of the defendants in this action. In it, General Hayden confirmed
26 the untargeted dragnet collection of communications records: “The first one was revealed through
27 revealing the FISA court order to Verizon. That’s about metadata and it’s about telephones. It’s
28 fact of call. And what happens there has been made now very clear by Director Clapper that the

1 United States government—the National Security Agency—is acquiring as business records, not
2 collecting on a wire anywhere, but acquiring as business records the metadata of foreign and
3 domestic phone calls here in the United States. And that constitutes billions of events per day.”
4 He continued: “So, NSA gets these records and puts them away, puts them in files.” “You put
5 these records, you store them, you have them. It’s kind of like, I’ve got the haystack now. And
6 now let’s try to find the needle.” He confirmed that the government does not obtain any further
7 FISC authorization when it searches its communications records database: “You have had a
8 generalized approval, and so you’ve got to justify the overall approach to the judge. But you do
9 not have to go to the judge, saying, hey, I got this number now. I’ll go ahead and get a FISA
10 request written up for you. No, you don’t have to do that.” Available at:

11 [http://www.npr.org/2013/06/09/190081216/ex-nsa-head-hayden-data-surveillance-balances-](http://www.npr.org/2013/06/09/190081216/ex-nsa-head-hayden-data-surveillance-balances-security-privacy)
12 [security-privacy.](http://www.npr.org/2013/06/09/190081216/ex-nsa-head-hayden-data-surveillance-balances-security-privacy)

13 9. Attached hereto as **Exhibit K** is the transcript of a June 9, 2013 Fox News interview
14 with General Hayden. In it, General Hayden confirmed the government was collecting “billions”
15 of communications records every day which the government stores indefinitely for later
16 examination—“you do retain the information so that you can ask questions of it in the future.”

17 Available at: [http://www.foxnews.com/on-air/fox-news-sunday-chris-](http://www.foxnews.com/on-air/fox-news-sunday-chris-wallace/2013/06/09/government-surveillance-unconstitutional-reaction-sens-rand-paul-ron-johnson-and-gen/print)
18 [wallace/2013/06/09/government-surveillance-unconstitutional-reaction-sens-rand-paul-ron-](http://www.foxnews.com/on-air/fox-news-sunday-chris-wallace/2013/06/09/government-surveillance-unconstitutional-reaction-sens-rand-paul-ron-johnson-and-gen/print)
19 [johnson-and-gen/print.](http://www.foxnews.com/on-air/fox-news-sunday-chris-wallace/2013/06/09/government-surveillance-unconstitutional-reaction-sens-rand-paul-ron-johnson-and-gen/print)

20 10. The following quotation is a true and correct transcription of testimony given by
21 Director of National Intelligence Clapper to the Senate three months ago before Congress. In his
22 March 12, 2013 testimony before the Senate Select Committee on Intelligence, the following
23 exchange occurred between Senator Ron Wyden and DNI Clapper:

24 Senator Wyden: “Last summer, the NSA Director was at a conference. And he was
25 asked a question about the NSA’s surveillance of Americans. He replied, and I
26 quote here, ‘The story that we have millions or hundreds of millions of dossiers on
27 people is completely false.’ The reason I’m asking the question is, having served on
28 the committee now for a dozen years, I don’t really know what a ‘dossier’ is in this
context. So, what I wanted to see is if you could give me a ‘yes’ or ‘no’ answer to
the question, Does the NSA collect any type of data at all on millions or hundreds of
millions of Americans?”

1 DNI Clapper: “No, sir.”

2 Senator Wyden: “It does not?”

3 DNI Clapper: “Not wittingly. There are cases where they could inadvertently
4 perhaps collect but not—not wittingly.”

5 Hearing before the Senate Select Committee on Intelligence (March 12, 2013). Video available at
6 the official Senate website:

7 <http://www.senate.gov/isvp/?comm=intel&type=live&filename=intel031213&stt=128:26&dur=135:15>.

8 Video also available at:

9 http://www.youtube.com/watch?feature=player_embedded&v=QwiUVUJmGjs#at=370.

10 Attached hereto as **Exhibit L** is a June 11, 2013 statement by Senator Wyden providing
11 further context for DNI Clapper’s statement at the March 12, 2013 hearing. Available at:

12 <http://www.wyden.senate.gov/news/press-releases/wyden-statement-responding-to-director-clappers-statements-about-collection-on-americans>.

14 11. The recent disclosures about the government’s electronic surveillance efforts
15 include reports of an NSA system called “PRISM” that facilitates collection of contents of emails
16 and other information created by users of Internet services such as Google, Facebook, and Yahoo.

17 Attached hereto as **Exhibit M** is a news story published June 6, 2013 by the *Guardian* describing
18 PRISM. Available at: <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

19 Attached hereto as **Exhibit N** is a news story published June 8, 2013 by the *Washington Post*
20 describing PRISM. Available at: [http://www.washingtonpost.com/world/national-security/us-](http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html)

21 [company-officials-internet-surveillance-does-not-indiscriminately-mine-](http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html)
22 [data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html](http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html). Attached hereto as

23 **Exhibit O** are slides from an NSA PowerPoint slide deck discussing PRISM published by the
24 *Washington Post* on June 6, 2013. Available at: [http://www.washingtonpost.com/wp-](http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/)
25 [srv/special/politics/prism-collection-documents/](http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/).

26 12. Attached hereto as **Exhibit P** is an NSA slide published June 8, 2013 by the
27 *Guardian* as part of the recent disclosures. Under the heading “Two Types of Collection” and the
28 subheading “Upstream,” the slide describes another surveillance capability in addition those used

1 for PRISM. This other surveillance capability is described as “Collection of communications on
2 fiber cables and infrastructure as data flows past.” Available at:
3 <http://www.guardian.co.uk/world/2013/jun/08/nsa-prism-server-collection-facebook-google>.

4 I declare under penalty of perjury under the laws of the United States that the foregoing is
5 true and correct to the best of my knowledge, information, and belief.

6 Executed at Palo Alto, CA on June 13, 2013.

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

s/ Thomas E. Moore III

Thomas E. Moore III

EXHIBIT A

TOP SECRET//SI//NOFORN

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 - 8 0

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

TOP SECRET//SI//NOFORN

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

TOP SECRET//SI//NOFORN

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)

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

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.

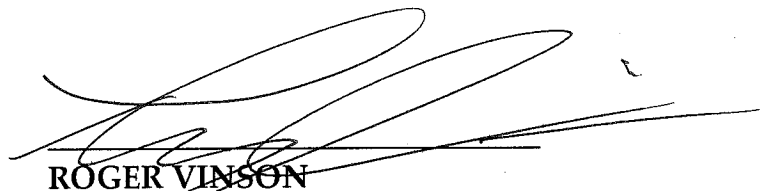
-- Remainder of page intentionally left blank. --

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN

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



ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

I, Beverly C. Queen, Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original. *BK*

TOP SECRET//SI//NOFORN

EXHIBIT B



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

DNI Statement on Recent Unauthorized Disclosures of Classified Information

June 6, 2013

DNI Statement on Recent Unauthorized Disclosures of Classified Information

The highest priority of the Intelligence Community is to work within the constraints of law to collect, analyze and understand information related to potential threats to our national security.

The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation.

The article omits key information regarding how a classified intelligence collection program is used to prevent terrorist attacks and the numerous safeguards that protect privacy and civil liberties.

I believe it is important for the American people to understand the limits of this targeted counterterrorism program and the principles that govern its use. In order to provide a more thorough understanding of the program, I have directed that certain information related to the "business records" provision of the Foreign Intelligence Surveillance Act be declassified and immediately released to the public.

The following important facts explain the purpose and limitations of the program:

- The judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation, on which members of Congress have been fully and repeatedly briefed. The classified program has been authorized by all three branches of the Government.
- Although this program has been properly classified, the leak of one order, without any context, has created a misleading impression of how it operates. Accordingly, we have determined to declassify certain limited information about this program.
- The program does not allow the Government to listen in on anyone's phone calls. The information acquired does not include the content of any communications or the identity of any subscriber. The only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls.
- The collection is broad in scope because more narrow collection would limit our ability to



DNI Statement on Recent Unauthorized Disclosures of Classified Information

screen for and identify terrorism-related communications. Acquiring this information allows us to make connections related to terrorist activities over time. The FISA Court specifically approved this method of collection as lawful, subject to stringent restrictions.

- The information acquired has been part of an overall strategy to protect the nation from terrorist threats to the United States, as it may assist counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities.
- There is a robust legal regime in place governing all activities conducted pursuant to the Foreign Intelligence Surveillance Act, which ensures that those activities comply with the Constitution and laws and appropriately protect privacy and civil liberties. The program at issue here is conducted under authority granted by Congress and is authorized by the Foreign Intelligence Surveillance Court (FISC). By statute, the Court is empowered to determine the legality of the program.
- By order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata acquired under the program. All information that is acquired under this program is subject to strict, court-imposed restrictions on review and handling. The court only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization. Only specially cleared counterterrorism personnel specifically trained in the Court-approved procedures may even access the records.
- All information that is acquired under this order is subject to strict restrictions on handling and is overseen by the Department of Justice and the FISA Court. Only a very small fraction of the records are ever reviewed because the vast majority of the data is not responsive to any terrorism-related query.
- The Court reviews the program approximately every 90 days. DOJ conducts rigorous oversight of the handling of the data received to ensure the applicable restrictions are followed. In addition, DOJ and ODNI regularly review the program implementation to ensure it continues to comply with the law.
- The Patriot Act was signed into law in October 2001 and included authority to compel production of business records and other tangible things relevant to an authorized national security investigation with the approval of the FISC. This provision has subsequently been reauthorized over the course of two Administrations – in 2006 and in 2011. It has been an important investigative tool that has been used over the course of two Administrations, with



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

DNI Statement on Recent Unauthorized Disclosures of Classified Information

the authorization and oversight of the FISC and the Congress.

Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions. Surveillance programs like this one are consistently subject to safeguards that are designed to strike the appropriate balance between national security interests and civil liberties and privacy concerns. I believe it is important to address the misleading impression left by the article and to reassure the American people that the Intelligence Community is committed to respecting the civil liberties and privacy of all American citizens.

James R. Clapper, Director of National Intelligence

###

EXHIBIT C



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

DIRECTOR JAMES R. CLAPPER INTERVIEW WITH

ANDREA MITCHELL, NBC NEWS CHIEF FOREIGN AFFAIRS CORRESPONDENT

LIBERTY CROSSING, TYSONS CORNER, VA

JUNE 8, 2013

1 P.M. EDT

Andrea Mitchell, NBC News Chief Foreign Affairs Correspondent: Director Clapper thank you very much for letting us come out here and interview you on the subject of all these leaks and how it has affected American intelligence gathering. Does the Intelligence Community feel besieged by the fact that these Top Secret documents are getting out?

James R. Clapper, Director of National Intelligence: Well I think we are very, very concerned about it. For me it is literally, not figuratively, literally, gut-wrenching to see this happen, because of the huge, grave damage it does to our intelligence capabilities. And of course, for me, this is a key tool for preserving and protecting the nation's safety and security. So, every one of us in the Intelligence Community most particularly the great men and women of NSA, are very – are profoundly affected by this.

Ms. Mitchell: How has it hurt American intelligence?

Director Clapper: Well, while we're having this debate, this discussion, and all this media explosion, which, of course, supports transparency -- which is a great thing in this country, but that same transparency has a double edged sword -- and that our adversaries, whether nation-state adversaries or nefarious groups – benefit from that transparency. So as we speak, they're going to school and learning how we do this. And so, that's why it potentially has -- can render great damage to our intelligence capabilities.

Ms Mitchell: At the same time, when Americans woke up and learned because of these leaks that every single telephone call made in the United States, as well as elsewhere, but every call made by these telephone companies that they collect is archived, the numbers, just the numbers and the duration of these calls, people were astounded by that. They had no idea. They felt invaded.

Director Clapper: I understand that. But first let me say that I and everyone in the Intelligence Community who are also citizens, who also care very deeply about our privacy and civil liberties, I certainly do. So let me say that at the outset. I think a lot of what people are reading



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

and seeing in the media is hyperbole. A metaphor I think might be helpful for people to understand this is to think of a huge library with literally millions of volumes of books in it, an electronic library. Seventy of those books are on bookcases in the United States, meaning that the bulk of the world's infrastructure, communications infrastructure, is in the United States. There are no limitations on the customers who can use this library. Many of millions of innocent people, doing millions of innocent things, use this library, but there are also nefarious people who use it -- terrorists, drug cartels, human traffickers, criminals also take advantage of the same technology. So the task for us in the interest of preserving security and preserving civil liberties and privacy, is to be as precise as we possibly can be. When we go in that library and look for the books that we need to open up and actually read, you think of them, and by the way, all these books are arranged randomly, they are not arranged by subject or topic matters, and they are constantly changing. And so when we go into this library first we have to have a library card, the people that actually do this work, which connotes their training and certification and recertification. So when we pull out a book, based on its essentially electronic Dewey Decimal System, which is zeros and ones, we have to be very precise about which books we are picking out, and if it is one that belongs or was put in there by an American citizen or a U.S. person, we are under strict court supervision, and have to get strict, have to get permission to actually look at that. So the notion that we're trolling through everyone's emails and voyeuristically reading them, or listening to everyone's phone calls is on its face absurd. We couldn't do it even if we wanted to, and I assure you, we don't want to.

Ms. Mitchell: Why do you need every telephone number? Why is it such a broad vacuum cleaner approach?

Director Clapper: Well, you have to start someplace. If and over the years this program has operated we have refined it and tried to make it ever more precise and more disciplined as to which things we take out of the library. But you have to be in the chamber in order to be able to pick and choose those things that we need in the interest of protecting the country, and gleaning information on terrorists who are plotting to kill Americans, to destroy our economy, and destroy our way of life.

Ms. Mitchell: Can you give me any examples where it has actually prevented a terror plot?

Director Clapper: Well, two cases that come to mind, which are a little dated, but I think in the interest of this discourse, should be shared with the American people, they both occurred in 2009, one was the aborted plot to bomb the subway in New York City in the fall of 2009. And this all started with a communication from Pakistan to a U.S. person in Colorado. And that led to the identification of a cell in New York City who was bent on a major explosion, bombing of the New York City subway. And a cell was rolled up and in their apartment we found backpacks with



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

bombs. A second example, also occurring in 2009, involved one of those involved, the perpetrators of the Mumbai bombing in India, David Headly. And we aborted a plot against a Danish news publisher based on the same kind of information. So those are two specific cases of uncovering plots through this mechanism that prevented terrorist attacks.

Ms Mitchell: Now Americans might say, "Yes, but terrorists succeeded in Boston at the marathon. Terrorists have succeeded elsewhere and not been thwarted despite all this information gathered by the NSA?"

Director Clapper: Right, Well, that's true and I find it a little ironic that several weeks ago after the Boston bombings, we were accused of not being sufficiently intrusive. We failed to determine the exact tipping point when the brothers self-radicalized. And then it was, we weren't intrusive enough. I don't mean to be a smart guy here, it's just emblematic of the serious debate that goes on in this country between the two poles of security, and civil liberties and privacy. And what we must, and I thought the President spoke really articulately about this yesterday in California. And he is exactly on the money. The challenge for us is navigating between these two poles. It's not a balance, it's not an either or. There has to be that balance so that we protect our country and also protect civil liberties and privacy.

Ms Mitchell: What the President said in part was that you can't have 100% security and then you have 100% privacy and zero inconvenience. We're going to have to make some choices as a society. There are accidents. NBC was told by one of your predecessors, Dennis Blair, that in fact, one digit was inaccurately inputted back in 2009 and it was a completely innocent person whose telephone conversations were actually eavesdropped.

Director Clapper: Right, there is no question, and I certainly wouldn't want to leave the impression that this process as complex and voluminous as it is, is perfect. Certainly it isn't. What we do try to do though is when errors are detected, and understand most of this is done through a computer process, it is not being done directly through human eyes and ears, but the computer processes are directed by humans and when we discover errors, which in all cases I am familiar with were innocent and unintended, they are immediately corrected and any of the ill begotten information is destroyed. And this is all done in response to court oversight and court direction.

Ms. Mitchell: There are people on the Hill who support your work strongly, Senator Feinstein among others, who say, "Can it be narrowed? Should we take another look at this and in fact, ask the FISA Court" -- the intelligence court last December during reauthorization debate -- "can you report back to the American people, periodically" and the court said, "No." The court operates without ex parte' and without any countervailing arguments doesn't it? Should that be



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

a cause of concern to Americans? Tell us why it should be in your view?

Director Clapper: Well certainly it should be a cause of concern to Americans, it is a cause of concern to us. And if we find ways, and we have found ways where we can refine these processes and limit the exposure to American's private communications, we will do that. In fact, Senator Feinstein has tasked us to look at such an innovation, specifically the NSA, and we owe her an answer in about a month. There are also, of course, people very, very concerned about civil liberties and privacy among whom for example, is Senator Wyden, whom I have great respect for. And he is passionate about civil liberties and privacy and he is averse to, and this gets to the second part of your question, averse to so-called secret law. Well, this gets to the issue of how openly these things are discussed. Because while transparency is good for our system, others less ideally motivated are taking advantage of that. Our perspective, from the Intelligence Community perspective, preserve and protect the secrecy because by exposing the tactics, techniques and procedures we use, our adversaries go to school on that and they make it even harder for us.

Ms. Mitchell: Senator Wyden made quite a lot out of your exchange with him last March during the hearings. Can you explain what you meant when you said there was not data collection on millions of Americans?

Director Clapper: First, as I said, I have great respect for Senator Wyden. I thought though in retrospect I was asked when are you going to start--stop beating your wife kind of question which is, meaning not answerable necessarily, by a simple yes or no. So I responded in what I thought was the most truthful or least most untruthful manner, by saying, "No." And again, going back to my metaphor, what I was thinking of is looking at the Dewey Decimal numbers of those books in the metaphorical library. To me collection of U.S. Persons data would mean taking the books off the shelf, opening it up and reading it.

Ms. Mitchell: Taking the content.

Director Clapper: Exactly, that's what I meant. Now...

Ms. Mitchell: You did not mean archiving the telephone numbers?

Director Clapper: No.

Ms. Mitchell: Let me ask you about the content.

Director Clapper: This has to do of course, somewhat of a semantic perhaps some would say



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

too cute by half, but there are honest differences on the semantics when someone says “collection” to me, that has a specific meaning, which may have a different meaning to him.

Ms Mitchell: Well, what do you say also, I should ask you what do you say to the other senators who are not on the committees? Not on the intelligence committees who have been invited in to read before these laws are reauthorized, and now are criticizing. Is there enough information available to the rest of the United States Senate and the rest of the members of Congress who are not expert when they go in before they vote?

Director Clapper: Well...

Ms. Mitchell: Do they know what they are voting on?

Director Clapper: I trust so. Obviously our primary two interlocutors are two intelligence oversight committees, both in the House and in the Senate. And so they are used to operating in a classified environment. Their staffs are, so that is primarily with whom we will do business. But on a piece of legislation say in this case the FISA Amendment Act, we provided detailed briefings and papers on this to explain the law, to explain the process it was governing. Now, I can't comment on whether senators and representatives were all able to avail themselves, but that material was made available and certainly if any member whether on the intelligence committee, the Judiciary Committee or any other committee would, who had asked for a specific briefing or follow up questions we certainly would respond, would have responded.

Ms. Mitchell: There were slides and details about the other programs. Programs on Internet providers. It has been referred to as “Prism” but technically it is 702 programs and according to The Washington Post report on that, it was a disgruntled intelligence officer who provided that Top Secret information to The Guardian and The Washington Post. How do you feel about that?

Director Clapper: Well, I think we all feel profoundly offended by that. This is someone who for whatever reason, has chosen to violate a sacred trust for this country. So we all look upon it no matter what his or her motivation may have been, the damage that these revelations incur are huge. And so I hope we are able to track down whoever is doing this because it is extremely damaging to, and it affects the safety and security of this country.

Ms. Mitchell: Can I assume from that, can I infer that there has been a referral to track down the leak?

Director Clapper: Absolutely. NSA has filed a crimes report on this already.



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

Ms. Mitchell: And some people would regard this person, he or she, as a whistleblower and a hero for letting the American public know that their emails are being tapped into and that their privacy is being invaded.

Director Clapper: There are legitimate outlets for anyone within the Intelligence Community who feels that some law is being violated, for reporting fraud, waste and abuse, and there are legitimate mechanisms for reporting that both within the Executive and in the Congress without damaging national security. And for whatever reason, a person or persons doing this chose not to use those legitimate outlets.

Ms. Mitchell: How do these programs work? Some of the Internet providers deny that they are cooperating so they seem to not be knowing.

Director Clapper: The Internet, the service providers – I'll speak generically – are doing this, but it is done under a court order and under legally mandated, legislatively mandated procedures. And it's, these are very precise, they're not indefinite and they have to be renewed and the court has to approve them.

Ms. Mitchell: The President and you and the others in this Top Secret world are saying, "Trust us. We have your best interest. We're not invading your privacy. We're going after bad guys. We're not going after your personal lives." What happens when you're gone, when this President or others in our government are gone? There could be another White House that breaks the law. There could be another DNI who does really bad things. We listened during the Watergate years to those tapes where the President of the United States saying, "Fire bomb the Brookings Institution." You know, what do you say to the American people about the next regime who has all these secrets? Do they live forever somewhere in a computer?

Director Clapper: No they don't live forever. That's a valid concern, I think. People come and go, Presidents come and go. Administrations come and go. DNIs will come and go. But what is, I think, important about our system is our system of laws, our checks and balances. You know, I think the Founding Fathers would actually be pretty impressed with how what they wrote, and the organizing principles for the country are still valid and are still used even to regulate a technology that they never foresaw. So that's timeless, those are part of our institutions. Are there people that will abuse these institutions? Yes, but we have a system that sooner or later, mostly sooner these days, those misdeeds are found out.

Ms Mitchell: And the data that are collected, do they live forever?

Director Clapper: No they do not. We...there are strict retention period limits, which are



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

overseen first by me, and the Attorney General, by the court system, and by the Congress, to ensure that the data collected is not held in perpetuity.

Ms. Mitchell: Now there's been another leak, in the last couple days. This one is another Top Secret order, ordering -- from the President -- ordering senior intelligence officials to draw up a list of potential overseas targets for cyber attack. How do you deal with a situation where there is a leak a day it seems of Top Secret information?

Director Clapper: Well, it's hard to deal with. It is again as in the case of this Presidential Directive an egregious violation of a sacred trust. That anyone who would have access to this would choose on his or her own, to violate that trust and disseminate this to the media. I would be surprised if anyone else were surprised if we weren't at least thinking about our behavior in the cyber domain. And so what this does is lay out a conceptual framework to include some definitions, for how we think about that.

Ms Mitchell: At a time when we're telling the Chinese you have invaded our businesses and our weapons systems, and you have to take responsibility for what's coming from your territory, don't these leaks undercut our arguments?

Director Clapper: Well they, perhaps, I think there is an understanding among nation states that we are going to monitor each others behavior. We do it. Other major nationstates do it as well. But I also think that there are limits, and just how aggressive that is and that's the reason for, I think, discussion among certainly industrialized nations for rules of the road for how we behave in cyber land.

Ms. Mitchell: We were told, NBC News reported that Senator John McCain during the campaign, had written a letter, a draft letter to the Taiwanese leader congratulating the new Taiwanese leader. And it was in the computer of his campaign. It hadn't been sent yet and he got a call from the Chinese government complaining about a letter that he had sent, that had not yet been sent to Taiwan, of course, China's acknowledged rival or enemy. How did that happen?

Director Clapper: Well, it happens because of the technology and the global nature of the Internet, and the connectivity that we all benefit from. But there are also downsides and this is a case in point. To me, what this illustrates is the importance of improved cyber security. A whole other subject. And also, the vulnerability that we all have when we use media of any form that is publically accessible.

Ms. Mitchell: I know what you're basically, your job is to stop the bad guys. To stop terrorist



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

attacks.

Director Clapper: Right.

Ms. Mitchell: And how much is that compromised by the current atmosphere of suspicion and criticism, and the feeling that the American public may not be supporting the effort in the future, and in the past has been very supportive?

Director Clapper: Well that's of great concern. That's of great concern to me, and all the Intelligence Community leadership that we cannot function without the support of the American people. We are, ourselves, part of the American people. And the vast majority of people in the Intelligence Community, whether military or civilian, take this as a point of honor, point of duty, of service to the country. They're not in it for the money, certainly, and they're not in it for the glorification. And so if people don't feel that way and don't trust the Intelligence Community to do the right thing, well that is a serious concern. And it is a serious personal concern of mine.

Ms. Mitchell: Do you know how many people had access to the Top Secret documents that were leaked to The Washington Post and The Guardian? Are we talking a handful? Hundreds?

Director Clapper: Well, I'd rather not go into that because that could kind of could impact the investigation that's going on. So I'd rather not answer that.

Ms. Mitchell: And are new procedures being put in to try to protect against this flow of leaks?

Director Clapper: Well, we've...we're constantly trying to institute new procedures. I'm in the process of attempting to institute some practices and policies that will try to stem the hemorrhaging of leaks, the leaking that we've had in recent years. But this is a tough problem because when it boils down to it, we operate -- even though we have clearances and we have SCIFs and secure areas -- when it all boils down to it, it is all about personal trust. And we've had violations of that personal trust in the past and we will continue to have them, and all we can do is learn lessons from when we find out what caused a revelation like this and make improvements and go on.

Ms. Mitchell: You know, a lot of this has to do with technology. Both the people's adaptation to it and the fear of it. We saw it in the Boston Marathon case how the number of cameras that were out there -- security cameras - private and government really did help. New York City is another instance. We get used to things like Homeland, a television series that apparently the President himself watches, with amazing technology. Is that the world we have to get used to?



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

LEADING INTELLIGENCE INTEGRATION

Director James R. Clapper Interview With Andrea Mitchell

Director Clapper: Well, I think it is and I think that you know, the pace of technology change, which by the way, poses a problem from both policy and a legal standpoint to keep up with rapid changes in technology, which is becoming ever more pervasive in our society. And you spoke of the surveillance cameras in Boston, which were crucial to tracking down the perpetrators, the two brothers. But at the same time, you know when you are on the Beltway and you have a radar gun that's looking at you and if you are under the speed limit you know you're not bothered. Photo cameras that take pictures of license plates and you get something in the mail saying you violated the speed limit. So those are all emblematic of today's society. The same providers who helped analyze our behavior, our purchasing behavior – well all of this is both an upside and a downside of this burgeoning technology.

Ms. Mitchell: Finally, your message to those who say, ACLU and others, we feel invaded, we don't know when you are looking at us or listening in on our conversations, and what is the real benefit? Why should we give up so much privacy? Can it be done better?

Director Clapper: We're trying to minimize those invasions of privacy and keep them to an absolute minimum and only focus on those targets that really do pose a threat and to not invade anyone's privacy, communications, telephone calls, emails if they are not involved in plotting against the United States. And so, as we, as the technologies changes that we were just talking about, we have to adapt as well to both provide that security and also ensure civil liberties and privacy.

Ms. Mitchell: Thank you very much Director Clapper.

Director Clapper: Thank you for having me.

EXHIBIT D

Transcript: Dianne Feinstein, Saxby Chambliss explain, defend NSA phone records program

By Ed O'Keefe, Updated: June 6, 2013

Sens. Dianne Feinstein (D-Calif.) and Saxby Chambliss (R-Ga.), who lead the Senate Intelligence Committee, spoke with reporters Thursday morning at a hastily arranged news conference to explain and defend the National Security Agency's collection of Verizon telephone records.

An unofficial transcript of the exchange appears below:

Sen. Dianne Feinstein: I just had an opportunity to review the Guardian article and I'd like to make the following points.

As far as I know, this is the exact three month renewal of what has been the case for the past seven years. This renewal is carried out by the FISA Court under the business records section of the Patriot Act. Therefore, it is lawful.

It has been briefed to Congress and the letters that we have distributed — and you'll note on the dates, this is prior to the Patriot Act amendments coming before the body, each of those. As you know, this is just metadata. There is no content involved. In other words, no content of a communication. That can only be, these records, I'm not talking about content, the records can only be accessed under heightened standards. The information goes into a database, the metadata, but cannot be accessed without what's called, and I quote, "reasonable, articulable suspicion" that the records are relevant and related to terrorist activity.

As you know, and I've pointed out many times, there have been approximately 100 plots and also arrests made since 2009 by the FBI. I do not know to what extent metadata was used or if it was used, but I do know this: That terrorists will come after us if they can and the only thing we have to deter this is good intelligence. To understand that a plot is being hatched and to get there before they get to us.

As you read those letters, you will see that they were sent at specific dates that were prior to each renewal of the particular business records section asking that members come and review in a classified session the data. That completes my statement.

Sen. Saxby Chambliss: Let me just emphasize, this is nothing particularly new. This has been going on for seven years under the auspices of the FISA authority and every member of the United States Senate has been advised of this.

To my knowledge, we have not had any citizen who has registered a complaint relative to the gathering of this information. It is simply what we call metadata that is never utilized by any

governmental agency unless they go back to the FISA court and show that there's real cause as to why something within the metadata should be looked at.

That's been very clear all along through the years of this program. It is proved meritorious, because we have gathered significant information on bad guys, but only on bad guys, over the years.

Question: Do you know how many of your Senate colleagues have actually looked at the classified information?

Feinstein: I do not. Certainly the Intelligence Committee should have. We've had long discussions. This has been argued on the floor. Mentioned in the article are two senators who've had concerns about it. Obviously when the second amendment came up there was considerable argument on the floor about this. The vote was taken and the measure passed and was continued. That's the business records section.

Question: To be clear: This isn't just Verizon, this is records generally with large phone records, right?

Feinstein: I can't specifically answer that, maybe David [Graniss, staff director of Senate Intelligence Committee]. Graniss, do you know?

David Graniss: We can't answer that question.

Feinstein: We cannot answer that. Fortunately, I don't know.

Question: One thing that has changed a lot since these letters is there's a climate that you feel more concerned about civil liberties, the IRS, drone strikes. Is it time to revisit some of the rules and measures you've put in place?

Feinstein: Let me put it from my point of view, and then the vice chairman will speak. I read intelligence carefully, and I know that people are trying to get to us. This is the reason why we keep TSA doing what it's doing. This is the reason why the FBI now has 10,000 people doing intelligence on counterterrorism. This is the reason for the National Counterterrorism Center that's been set up in the time we've been active. It's to ferret this out before it happens. It's called protecting America.

Look, I'm concerned about the use of drones as much as anybody, and with some degree of knowledge as to how they're used. We are trying to put something together in an authorization bill to deal with this, but that's a ways, a month or so, off right now. One doesn't necessarily follow the other. I think people want the homeland kept safe, to the extent we can. We understand — I understand — privacy. Senator Chambliss understands privacy. We want to protect people's private rights. And that's why this is carefully done. That's why it's a federal court of 11 judges who sit 24/7, who review these requests and then either approves them or denies them.

Chambliss: Let me just add to what the chairman said. The Intelligence Committee takes its oversight authority and obligation very seriously. We review every program within the intelligence community on a regular basis, including this program. That's why we took the liberty of explaining to our colleagues the substance of the program in the two "Dear Colleagues" that we handed out. And we're going to continue to do that. Where we find abuses, we're going to take corrective action.

Question: Do you guys know what the information is being used for? What is the government doing with the information?

Feinstein: If there is reasonable, articulable belief that this metadata would figure in a terrorist investigation, then they can examine it. Phone numbers.

Question: Why does it need to be so sweeping? What possible investigation could require all of the phone records?

Feinstein: Well, because they then have what's a telephone book of the numbers and if, through another way, information comes to the FBI that there is reasonable suspicion that a terrorist act, conspiracy, planning, carrying out, is going on, they can access those records. The records are there to access. This is not something, I think, that we don't view with extraordinary caution. We do. As you know, both Senator Wyden and Senator Udall have concerns. This was widely debated on the floor when the section of the code was discussed. It was widely debated in the Intelligence Committee when we considered the business records section. So this is simply, it's renewed every three months, they must go into court, and this is that renewal.

Question: Is it true, then, that this data has been used proactively to have as a hold, so that they'll have this data in case they want to research and go through it later ... as opposed to looking for something specific and then asking for the data? They're getting this data so they'll have it so that they can go back to it if they need it?

Feinstein: I have to get for you the information, because this just came up a few minutes ago, how long the data can be kept.

Question: But they're sort of logging this data so they can hold it if they need it later, as opposed to knowing that they need it and getting it.

Feinstein: Well, you can't know that you need it at the time. You have to go to it and see if there is the link that you're looking for.

Chambliss: The information that they're really looking for is on the other end of the call. It's: Are they in contact, is somebody in contact with somebody that we know to be a known terrorist? And that's why it's metadata only and it's what we call minimized. All these numbers are basically ferreted out by computer, but if there's a number that matches a terrorist number that has been dialed by a U.S. number or dialed from a terrorist to a U.S. number, then that may be flagged. And they may or may not seek a court order to go further on that particular instance. But that's the only time that this information is ever used in any kind of substantive way.

Feinstein: That is our understanding I'm glad you said that, thank you. That is our understanding.

Question: You say this is not new. All of us were here when you debated reauthorizing FISA a few weeks ago. What is new is that it's now public. Should there be an investigation into who leaked this information?

Feinstein: Well, you have to give me a little time. I first saw this maybe an hour ago, so I haven't had an opportunity to do due diligence and I assume that the same is true for Senator Chambliss.

We will put out a joint statement.

(End of press conference)

Share your thoughts in the comments section below.

© The Washington Post Company

EXHIBIT E

- [CBSNews.com](#) • [CBS Evening News](#) • [CBS This Morning](#) • [48 Hours](#) • [60 Minutes](#) • [Sunday Morning](#) • [Face the Nation](#)
- [Video](#) • [US](#) • [World](#) • [Politics](#) • [Entertainment](#) • [Health](#) • [MoneyWatch](#) • [SciTech](#) • [Crime](#) • [Sports](#) • [More](#)
- [Log](#)



By
 Stephanie Condon /
 CBS News/ June 6, 2013, 1:51 PM

NSA's Verizon records collection: "Calm down," Reid says

• [491 Comments](#) • [2K Shares](#) • [129 Tweets](#) • [Stumble](#) • [Email](#) • [More +](#) *Updated at 5:43 p.m. ET*

The National Security Agency's blanket request for Verizon to hand over all records of telephone calls within its system -- both within the U.S. and between the U.S. and other countries -- was a routine request made under congressionally-approved laws, Senate Majority Leader Harry Reid, D-Nev., and some other members of Congress insisted Thursday.

"Right now I think everyone should just calm down and understand that this isn't anything that is brand new, it's been going on for some seven years, and we have tried to often to try to make it better and work and we will continue to do that," Reid told reporters, referring to the surveillance protocols put in place by the updated Foreign Intelligence Surveillance Act (FISA) and the Patriot Act.

- [Report: Feds getting phone records of all Verizon customers](#)

Sen. Saxby Chambliss, R-Ga., vice chairman of the Senate Intelligence Committee, concurred with Reid, commenting, "This is nothing particularly new."

"This has been going on for seven years under the auspices of the FISA authority and every member of the United States Senate has been advised of this," he said.

Other members of Congress, however -- including one of the authors of the Patriot Act, Rep. Jim Sensenbrenner, R-Wis. -- expressed outrage and concern about the data collection.





[Play Video](#)

Miller: NSA collecting data, not listening in on Americans



[Play Video](#)

Graham: Verizon giving data to government "doesn't bother me one bit"

"As the author of the Patriot Act, I am extremely disturbed by what appears to be an overbroad interpretation of the Act," Sensenbrenner said in a letter sent Thursday to Attorney General Eric Holder. Sensenbrenner said the Patriot Act was intended to balance national security and civil rights, but he has "always worried about potential abuses."

As first reported by the Guardian newspaper in Britain, the secret Foreign Intelligence Surveillance Court granted a request from the NSA and the FBI to collect the Verizon data from a three-month period ending on July 19. The order was granted under the so-called "business records" provision of the Patriot Act, though Sensenbrenner pointed out in his letter to Holder that the provision requires the government to prove the relevancy of the information and meet certain thresholds before acquiring business records, especially with respect to records pertaining to U.S. citizens.

Sensenbrenner said he doesn't believe the FISA order meets those standards. "How could the phone records of so many innocent Americans be relevant to an authorized investigation?" he asked in the letter. He asked Holder to explain why the request was so broad and whether the FBI believes there are any limits to the information they can obtain from the Patriot Act's "business records" provision.

Other members of Congress, meanwhile, expressed concern over whether the executive branch could be monitoring members of Congress or the Supreme Court. If members of the executive branch were monitoring telephone records from Congress, Sen. Mark Kirk, R-Ill., said Thursday, it "would give them unique leverage over the legislature." Kirk expressed this concern directly to Holder, who was testifying about the Justice Department's budget in a Senate Appropriations Committee hearing.

Holder said he could brief the committee in a closed-door session later, given the sensitive nature of the subject. Kirk retorted, "The correct answer would be to say no, we stayed within our lane, and I'm assuring you we did not spy on members of Congress."

Sen. Barbara Mikulski, D-Md., head of the Appropriations Committee, told Holder that the full Senate -- not just the Intelligence Committee -- should be briefed on the surveillance. "I will send a note to [Democratic and Republican leaders] Reid and McConnell because I think this cuts across committees," she said. "I think it goes to Judiciary. I think it goes to Armed Services. I think it goes to intel."

-
-

1/2

© 2013 CBS Interactive Inc. All Rights Reserved.

- [491 Comments](#)
- [2K Shares](#)
- [129 Tweets](#)
- [Stumble](#)
- [Email](#)
- [More +](#)
- [Stephanie Condon On Twitter »](#)

Stephanie Condon is a political reporter for CBSNews.com.

Around the Web

- [TV Weather Star Dealing with MS Diagnosis](#)lifescript.com
- [Why Shampoos Are a Waste of Money](#)knoworthy.com
- [50 Shades of Grey Movie Cast](#)popsugar.com
- [4 Things You'll Feel Right Before a Heart Attack](#)Newsmax.com

[CBSNews.com](#) [CBS Evening News](#) [CBS This Morning](#) [48 Hours](#) [60 Minutes](#) [Sunday Morning](#) [Face the Nation](#)

[Video](#) [US](#) [World](#) [Politics](#) [Entertainment](#) [Health](#) [MoneyWatch](#) [SciTech](#) [Crime](#) [Sports](#) [More](#)

[Log](#)

By
Stephanie Condon /
CBS News/ June 6, 2013, 1:51 PM

NSA's Verizon records collection: "Calm down," Reid says

[491 Comments](#)

[7 Shares](#) [129 Tweets](#) [Stumble](#) [Email](#) [More +](#)

Like Chambliss, other members of Congress who receive intelligence briefings

said the surveillance was appropriate -- and very useful. House Intelligence Committee Chairman Mike Rogers, R-Mich., said Thursday that the program the NSA used in this Verizon case did stop a terrorist attack in the past.



[Play Video](#)

Rogers: Giving call data to NSA has already stopped a terror attack

"Within the last few years, there was a domestic case that was thwarted because of their ability to do this," he said. "It's used to make sure there is not an international nexus to any terrorism event they may believe is ongoing in the United States."

Sen. Dianne Feinstein, D-Calif., chairwoman of the Senate Intelligence Committee, went even further, saying multiple plots were thwarted. "There were terrorists plots in the plural, let me put it that way," she said.

While Rogers said the FISA court order does not appear to be anything unusual, he said the intelligence committee will review whether it is legal and that they would begin conversations with the "relevant players" Thursday afternoon.

Chambliss pointed out that the NSA and FBI were only collecting data such as the dates and times of calls -- they were not monitoring the substance of calls. "To my knowledge, we have not had any citizen who has registered a complaint relative to the gathering of this information, and it is simply metadata that is never utilized by any governmental agency unless they go back to the FISA court and show that there is real cause as to why something within the metadata should be looked at," he said.

While the collection of the data may be legal, some members of Congress said it violated the spirit of the Constitution and the public's expectations of privacy.

"I believe that when law-abiding Americans call their friends, who they call, when they call, and where they call from is private information," Sen. Ron Wyden, D-Ore., a senior member of the Senate Intelligence committee, said in a statement. "Collecting this data about every single phone call that every American makes every day would be a massive invasion of Americans' privacy."

Wyden said that based on his several years of intelligence oversight, the value and effectiveness of such programs "remain unclear" to him. "The American people have a right to know whether their government thinks that the sweeping, dragnet surveillance that has been alleged in this story is allowed under the law and whether it is actually being conducted," he said.

Sen. Rand Paul, R-Ky., called the surveillance "an astounding assault on the Constitution." He noted that he and Sen. Mike Lee, R-Utah last year tried to amend FISA to increase Fourth Amendment protections, but the measure was defeated.

"If the President and Congress would obey the Fourth Amendment we all swore to uphold, this new shocking revelation that the government is

now spying on citizens' phone data en masse would never have happened," he said.

-
-

2/2

© 2013 CBS Interactive Inc. All Rights Reserved.

- [491 Comments](#)
- [Shares](#)
- [129 Tweets](#)
- [Stumble](#)
- [Email](#)
- More +
 - [Stephanie Condon On Twitter »](#)

Stephanie Condon is a political reporter for CBSNews.com.

Around the Web

- [TV Weather Star Dealing with MS Diagnosis](#) [lifescript.com](#)
- [Why Shampoos Are a Waste of Money](#) [knowworthy.com](#)
- [50 Shades of Grey Movie Cast](#) [popsugar.com](#)
- [34 Hottest Rachel McAdams Pictures of All Time](#) [ranker.com](#)

What's this?

Popular in Politics

- [Snowden's NSA leak an "act of treason," says Democratic senator](#) [Sens. Nelson and Chambliss call for Edward Snowden to be extradited for leaking documents from top-secret government surveillance programs](#)
- [Feds to comply with NY morning-after pill ruling on age limits](#) [Brooklyn judge ordered earlier this year that "morning after" pill be made available to all ages without prescription](#)
- [What drove Obama's change of heart on government snooping?](#) [185 Comments](#)
- [Man claiming to be NSA whistleblower comes forward](#) [953 Comments](#)
- [State Dept. dismisses allegations of "endemic" misconduct](#)

EXHIBIT F

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format.

Order a reprint of this article now

THE WALL STREET JOURNAL.

WSJ.com

POLITICS | Updated June 7, 2013, 9:25 a.m. ET

U.S. Collects Vast Data Trove

NSA Monitoring Includes Three Major Phone Companies, as Well as Online Activity

By [SIOBHAN GORMAN](#), [EVAN PEREZ](#) and [JANET HOOK](#)

WASHINGTON—The National Security Agency's monitoring of Americans includes customer records from the three major phone networks as well as emails and Web searches, and the agency also has cataloged credit-card transactions, said people familiar with the agency's activities.



Jerry Seib explains how the far-reaching data collection conducted by the U.S. government includes phone companies in addition to Verizon, plus Internet service providers and Apple. Photo: Getty Images



The Obama administration says its review of complete phone records of U.S. citizens is a "necessary tool" in protecting the nation from terror threats. Is this the accepted new normal, or has the Obama administration pushed the bounds of civil liberties? Cato Institute Director of Information Policy Studies Jim Harper weighs in. Photo: Getty Images.

The disclosure this week of an order by a secret U.S. court for [Verizon Communications Inc.](#)'s phone records set off the latest public discussion of the program. But people familiar with the NSA's operations said the initiative also encompasses phone-call data from [AT&T Inc.](#) and [Sprint Nextel Corp.](#), records from Internet-service providers and purchase information from credit-card providers.

The agency is using its secret access to the communications of millions of Americans to target possible terrorists, said people familiar with the effort.

The NSA's efforts have become institutionalized—yet not so well known to the public—under laws passed in the wake of the Sept. 11, 2001, attacks. Most members of Congress defended them Thursday as a way to root out terrorism, but civil-liberties groups decried the program.

"Everyone should just calm down and understand this isn't anything that is brand new," said Senate Majority Leader [Harry Reid](#) (D., Nev.), who added that the phone-data program has "worked to prevent" terrorist attacks.

Senate Intelligence Chairman [Dianne Feinstein](#) (D., Calif.) said the program is lawful and that it must be renewed by the secret U.S. court every three months.

Vote and comment

She said the revelation about Verizon, reported by the London-based newspaper the Guardian, seemed to coincide with its latest renewal.

Civil-liberties advocates slammed the NSA's actions. "The most recent surveillance program is breathtaking. It shows absolutely no effort to narrow or tailor the surveillance of citizens," said Jonathan Turley, a constitutional law expert at George Washington University.



The National Security Agency is obtaining phone records from all Verizon U.S. customers under a secret court order, according to a newspaper report and ex-officials. WSJ intelligence correspondent Siobhan Gorman joins MoneyBeat. Photo: AP.

Meanwhile, the Obama administration acknowledged Thursday a secret NSA program dubbed Prism, which a senior administration official said targets only foreigners and was authorized under U.S. surveillance law. The Washington Post and the Guardian reported earlier Thursday the existence of the previously undisclosed program, which was described as providing the NSA and FBI direct access to server systems operated by tech companies that include [Google Inc.](#), [Apple Inc.](#), [Facebook Inc.](#), [Yahoo Inc.](#), [Microsoft Corp.](#) and Skype. The newspapers, citing what they said was an internal NSA document, said the agencies received the contents of emails, file transfers and live chats of the companies' customers as part of their surveillance activities of foreigners whose activity online is routed through the U.S. The companies mentioned denied knowledge or participation in the program.

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. The practice, which evolved out of warrantless wiretapping programs begun after 2001, is now approved by all three branches of the U.S. government.

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.

NSA also obtains access to data from Internet service providers on Internet use such as data about email or website visits, several former officials said. NSA has established similar relationships with credit-card companies, three former officials said.

All Things D

[The Laws That Make It Easy for the Government to Spy on Americans](#)

More

[What the NSA Wants to Know About You and Your Phone](#)

[Tech Companies' Data Is Also Tapped](#)

[FISA Court in Focus](#)

[Obama's Civil-Liberties Record Questioned](#)

[When NSA Calls, Companies Answer](#)

[Mixed Reactions on Hill](#)

[Lawmakers Push Holder for Briefing on Phone Records | \[More Reaction\]\(#\)](#)

[Verizon Says Must Comply with Data Requests](#)

[Government Is Tracking Verizon Calls](#)

[NSA's Domestic Spying Grows as Agency Sweeps Up Data \(3/10/2008\)](#)

[NSA Exceeds Legal Limits in Eavesdropping Program \(4/16/2009\)](#)

[U.S. Plans 'Perfect Citizen' Cyber Shield for Utilities, Companies \(7/8/2010\)](#)

[NSA Activities Violated Fourth Amendment Rights, Letter Discloses \(7/20/2012\)](#)



From the Archives

More

[Video: U.S. Data Gathering Highlights Carriers' Balancing Act](#)

[Video: U.S. Tracks Verizon Calls: A Lawyer's Take](#)

But the disconnect between the program's supporters and detractors underscored the difficulty Congress has had navigating new technology, national security and privacy.

The Obama administration, which inherited and embraced the program from the George W. Bush administration, moved Thursday to forcefully defend it. White House spokesman Josh Earnest called it "a critical tool in protecting the nation from terror threats."

But Sen. Ron Wyden (D., Ore.), said he has warned about the breadth of the program for years, but only obliquely because of classification restrictions.

"When law-abiding Americans call their friends, who they call, when they call, and where they call from is private information," he said. "Collecting this data about every single phone call that every American makes every day would be a massive invasion of Americans' privacy."

In the wake of the Sept. 11 attacks, phone records were collected without a court order as a component of the Bush-era warrantless surveillance program authorized by the 2001 USA Patriot Act, which permitted the collection of business records, former officials said.

The ad hoc nature of the NSA program changed after the Bush administration came under criticism for its handling of a separate, warrantless NSA eavesdropping program.

President Bush acknowledged its existence in late 2005, calling it the Terrorist Surveillance Program, or TSP.

When Democrats retook control of Congress in 2006, promising to investigate the administration's counterterrorism policies, Bush administration officials moved to formalize court oversight of the NSA programs, according to former U.S. officials.

Congress in 2006 also made changes to the Patriot Act that made it easier for the government to collect phone-subscriber data under the Foreign Intelligence Surveillance Act.

Those changes helped the NSA collection program become institutionalized, rather than one conducted only under the authority of the president, said people familiar with the program.

Along with the TSP, the NSA collection of phone company customer data was put under the jurisdiction of a secret court that oversees the Foreign Intelligence Surveillance Act, according to

It couldn't be determined if any of the Internet or credit-card arrangements are ongoing, as are the phone company efforts, or one-shot collection efforts. The credit-card firms, phone companies and NSA declined to comment for this article.

Though extensive, the data collection effort doesn't entail monitoring the content of emails or what is said in phone calls, said people familiar with the matter. Investigators gain access to so-called metadata, telling them who is communicating, through what medium, when, and where they are located.

But the disconnect between the program's supporters and detractors underscored the difficulty Congress has had navigating new technology, national security and privacy.

The Obama administration, which inherited and embraced the program from the George W. Bush administration, moved Thursday to forcefully defend it. White House spokesman Josh Earnest called it "a critical tool in protecting the nation from terror threats."

But Sen. Ron Wyden (D., Ore.), said he has warned about the breadth of the program for years, but only obliquely because of classification restrictions.

"When law-abiding Americans call their friends, who they call, when they call, and where they call from is private information," he said. "Collecting this data about every single phone call that every American makes every day would be a massive invasion of Americans' privacy."

In the wake of the Sept. 11 attacks, phone records were collected without a court order as a component of the Bush-era warrantless surveillance program authorized by the 2001 USA Patriot Act, which permitted the collection of business records, former officials said.

The ad hoc nature of the NSA program changed after the Bush administration came under criticism for its handling of a separate, warrantless NSA eavesdropping program.

President Bush acknowledged its existence in late 2005, calling it the Terrorist Surveillance Program, or TSP.

When Democrats retook control of Congress in 2006, promising to investigate the administration's counterterrorism policies, Bush administration officials moved to formalize court oversight of the NSA programs, according to former U.S. officials.

Congress in 2006 also made changes to the Patriot Act that made it easier for the government to collect phone-subscriber data under the Foreign Intelligence Surveillance Act.

Those changes helped the NSA collection program become institutionalized, rather than one conducted only under the authority of the president, said people familiar with the program.

Along with the TSP, the NSA collection of phone company customer data was put under the jurisdiction of a secret court that oversees the Foreign Intelligence Surveillance Act, according to

officials.

David Kris, a former top national security lawyer at the Justice Department, told a congressional hearing in 2009 that the government first used the so-called business records authority in 2004.

At the time he was urging the reauthorization of the business-records provisions, known as Section 215 of the Patriot Act, which Congress later approved.

The phone records allow investigators to establish a database used to run queries when there is "reasonable, articulable suspicion" that the records are relevant and related to terrorist activity, Ms. Feinstein said Thursday.

Director of National Intelligence James Clapper also issued a defense of the phone data surveillance program, saying it is governed by a "robust legal regime." Under the court order, the data can only "be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." When the data is searched, all information acquired is "subject to strict restrictions on handling" overseen by the Justice Department and the surveillance court, and the program is reviewed roughly every 90 days, he said. Another U.S. official said less than 1% of the records are accessed.

The database allows investigators to "map" individuals connected with that information, said Jeremy Bash, who until recently was chief of staff at the Pentagon and is a former chief counsel to the House Intelligence committee.

"We are trying to find a needle in a haystack, and this is the haystack," Mr. Bash said, referring to the database.

Sen. Wyden on Thursday questioned whether U.S. officials have been truthful in public descriptions of the program. In March, Mr. Wyden noted, he questioned Mr. Clapper, who said the NSA did not "wittingly" collect any type of data pertaining to millions Americans. Spokesmen for Mr. Clapper didn't respond to requests for comment.

For civil libertarians, this week's disclosure of the court authorization for part of the NSA program could offer new avenues for challenges. Federal courts largely have rebuffed efforts that target NSA surveillance programs, in part because no one could prove the information was being collected. The government, under both the Bush and Obama administrations, has successfully used its state-secrets privilege to block such lawsuits.

Jameel Jaffer, the American Civil Liberties Union's deputy legal director, said the fact the FISA court record has now become public could give phone-company customers standing to bring a lawsuit.

"Now we have a set of people who can show they have been monitored," he said.

—Danny Yadron
and Jennifer Valentino-DeVries
contributed to this article.

Corrections & Amplifications

The NSA monitoring program must be approved by a secret U.S. court every three months. An earlier version of this article incorrectly the approval came from Congress.

Write to Siobhan Gorman at siobhan.gorman@wsj.com, Evan Perez at evan.perez@wsj.com and

Janet Hook at janet.hook@wsj.com

A version of this article appeared June 7, 2013, on page A1 in the U.S. edition of The Wall Street Journal, with the headline: U.S. Collects Vast Data Trove.

Copyright 2012 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

EXHIBIT G

F. JAMES SENSENBRENNER, JR.

FIFTH DISTRICT, WISCONSIN

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON
CRIME, TERRORISM, AND
HOMELAND SECURITY
CHAIRMANCOMMITTEE ON SCIENCE, SPACE,
AND TECHNOLOGY
VICE-CHAIRMAN

Congress of the United States
House of Representatives
Washington, DC 20515-4905

WASHINGTON OFFICE:

ROOM 2449

RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-4905
202-225-5101

DISTRICT OFFICE:

120 BISHOPS WAY, ROOM 154
BROOKFIELD, WI 53005-6294
262-784-1111

OUTSIDE MILWAUKEE METRO

CALLING AREA:

1-800-242-1119

WEBSITE:

[HTTP://SENSENBRENNER.HOUSE.GOV](http://SENSENBRENNER.HOUSE.GOV)

June 6, 2013

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Holder:

As the author of the Patriot Act, I am extremely disturbed by what appears to be an overbroad interpretation of the Act. The Federal Bureau of Investigations (FBI) applied for a top secret court order to collect the phone records of virtually every call that has been made by millions of Verizon customers. These reports are deeply concerning and raise questions about whether our constitutional rights are secure.

The Patriot Act was a careful balancing of national security interests and constitutional rights. While I believe we found an appropriate balance, I have always worried about potential abuses of the Act.

The FBI's broad application for phone records was made under section 215—the so-called business records provision—of the Act. To obtain a business records order from the court, the Patriot Act requires the government to show that: (1) it is seeking the information in certain authorized national security investigations conducted pursuant to guidelines approved by the Attorney General;¹ (2) if the investigative target is a U.S. person, the investigation is not based solely on activities protected by the First Amendment;² and (3) the information sought is relevant to the authorized investigation.³ In addition, the Patriot Act requires the government to adhere to minimization procedures that limit the retention and dissemination of the information that is obtained concerning U.S. persons.⁴

I insisted upon sunseting this provision in order to ensure Congress had an opportunity to reassess the impact the provision had on civil liberties. I also closely monitored and relied on

¹ 50 U.S.C. § 1861(a)(2)(A).

² *Id.* at § (a)(1), (a)(2)(B).

³ *Id.* at § (b)(2)(A).

⁴ *Id.* at § 1861(b)(2)(B) and (g).

testimony from the Administration about how the Act was being interpreted to ensure that abuses had not occurred. On March 9, 2011, Acting Assistant Attorney General Todd Hinnen told the Judiciary Committee:

Section 215 has been used to obtain driver's license records, hotel records, car rental records, apartment leasing records, credit card records, and the like. It has never been used against a library to obtain circulation records. . . On average, we seek and obtain section 215 orders less than 40 times per year.⁵

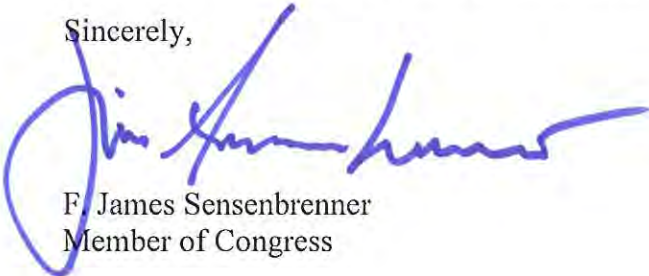
The Department's testimony left the Committee with the impression that the Administration was using the business records provision sparingly and for specific materials. The recently released FISA order, however, could not have been drafted more broadly.

I do not believe the released FISA order is consistent with the requirements of the Patriot Act. How could the phone records of so many innocent Americans be relevant to an authorized investigation as required by the Act? Please respond to the following questions by June 12, 2013:

1. Do you believe that the recently released FISA order is consistent with the requirements of the Patriot Act?
2. Why was the order so broad?
3. Is the released FISA order consistent with the FBI's interpretation of section 215 of the Patriot Act?
4. Does the FBI believe there are limits on what information it can obtain under section 215? If so, what are those limits?

Section 215 is an urgent tool and crucial to intelligence agencies, but if such abuses are not reined in, it will be very difficult to reauthorize these provisions when they sunset in 2015. Thank you for your prompt and personal response to this serious matter.

Sincerely,



F. James Sensenbrenner
Member of Congress

⁵ Statement of Todd Hinnen, Acting Assistant Attorney General for National Security, House Judiciary Subcommittee on Crime, Terrorism and Homeland Security (March 9, 2011).

EXHIBIT H

This abuse of the Patriot Act must end

President Obama falsely claims Congress authorised all NSA surveillance. In fact, our law was designed to protect liberties



Jim Sensenbrenner

guardian.co.uk, Sunday 9 June 2013 07.00 EDT



Barack Obama discusses the NSA surveillance controversy at a press conference in California, on Friday. Photograph: Evan Vucci/AP

We've gotten used to what "Big Government" looks like – Washington's unchecked deficit spending, the Obama administration's policing of the press and the IRS's targeting of conservative groups. But the problem is bigger than we thought. "Big Brother" is watching. And he is monitoring the phone calls and digital communications of every American, as well as of any foreigners who make or receive calls to or from the United States.

Last week, the Guardian reported that the Obama administration is collecting records of every call made to, from or within the US, as well as records of many digital communications. President Obama has tried to deflect criticism by claiming "every member of Congress has been briefed on this program." While some members of

Congress were briefed – particularly those on the intelligence committees – most, including myself, were not.

The administration claims authority to sift through details of our private lives because the Patriot Act says that it can. I disagree. I authored the Patriot Act, and this is an abuse of that law.

I was the chairman of the House judiciary committee when the US was attacked on 11 September 2001. Five days later, the Justice Department delivered its proposal for new legislation. Although I, along with every other American, knew we had to strengthen our ability to combat those targeting our country, this version went too far. I believed then and now that we can defend our country and our liberty at the same time.

I immediately called then-House Speaker Dennis Hastert and asked him for time to redraft the legislation. I told the speaker that if the legislation moved forward as drafted, I would not only vote against it, but would actively oppose it.

The country wanted action, and the pressure from the White House was intense. To his credit, Speaker Hastert gave us more time. There were endless meetings and non-stop negotiations with the White House, the FBI and the intelligence community. The question could not have been more fundamental: how could we defend our liberty and protect the American people at the same time?

The legislation had to be narrowly tailored – everyone agreed that we could not allow unrestrained surveillance. The Patriot Act had 17 provisions. To prevent abuse, I insisted on sunseting all the provisions so that they would automatically expire if Congress did not renew them. This would allow Congress to conduct oversight of the administration's implementation of the act.

In 2006, Congress made 14 of the provisions permanent because they were noncontroversial. The three remaining provisions, including the so-called business records provision the administration relied on for the programs in question, will expire in 2015 if they are not reauthorized.

The final draft was bipartisan and passed the judiciary committee unanimously. The Patriot Act has saved lives by ensuring that information is shared among those responsible for defending our country and by giving the intelligence community the tools it needs to identify and track terrorists.

In his press conference on Friday, President Obama described the massive collection of phone and digital records as "two programs that were originally authorized by Congress, have been repeatedly authorized by Congress". But Congress has never specifically authorized these programs, and the Patriot Act was never intended to allow

the daily spying the Obama administration is conducting.

To obtain a business records order like the one the administration obtained, the Patriot Act requires the government to prove to a special federal court, known as a Fisa court, that it is complying with specific guidelines set by the attorney general and that the information sought is relevant to an authorized investigation. Intentionally targeting US citizens is prohibited.

Technically, the administration's actions were lawful insofar as they were done pursuant to an order from the Fisa court. But based on the scope of the released order, both the administration and the Fisa court are relying on an unbounded interpretation of the act that Congress never intended.

The released Fisa order requires daily productions of the details of every call that every American makes, as well as calls made by foreigners to or from the United States. Congress intended to allow the intelligence communities to access targeted information for specific investigations. How can every call that every American makes or receives be relevant to a specific investigation?

This is well beyond what the Patriot Act allows.

President Obama's claim that "this is the most transparent administration in history" has once again proven false. In fact, it appears that no administration has ever peered more closely or intimately into the lives of innocent Americans. The president should immediately direct his administration to stop abusing the US constitution.

We all know the saying "eternal vigilance is the price of liberty." We are seeing that truth demonstrated once again.

Our liberties are secure only so long as we are prepared to defend them. I and many other members of Congress intend to take immediate action to ensure that such abuses are not repeated.

More from the Guardian [What's this?](#)

[There's a right way to deal with hecklers. Then there's Michelle Obama's...](#) 09 Jun 2013

[Pursuit of Happiness radio show couple found dead in New York](#) 07 Jun 2013

[Edward Snowden: the whistleblower behind the NSA surveillance revelations](#) 09 Jun 2013

[I despair as I watch the erosion of the liberal views I hold dear](#) 09 Jun 2013

More from around the web [What's this?](#)

[Rare WWII Plane Takes Flight in New Orleans](#) (Yahoo!)

[6 Markets that Will Rule the Next Decade](#) (Business Without Borders)

[A kitchen remodel for under \\$5k](#) (HomeGoods)

[HIPPA and the BYOD Challenge](#) (Moss Adams)

EXHIBIT I

THE WALL STREET JOURNAL.

WSJ.com

June 7, 2013, 1:13 PM ET

Transcript: Obama's Remarks on NSA Controversy

Video: Obama discusses the data collection efforts.

President Barack Obama on Friday [defended his administration's vast data-collection efforts](#), saying the programs help prevent terrorist attacks and represent only small encroachments of people's privacy. Here is the transcript of his remarks, which he made at the end of a planned speech on the new health law.

Transcript provided by Federal News Service (www.fednews.com)

PRESIDENT OBAMA: I'm going to take one question. And then remember, people are going to have opportunity to — I'll also answer questions when I'm with the Chinese president today. So I don't want the whole day to just be a bleeding press conference. But I'm going to take Jackie Calmes's question.

Q: Mr. President, could you please react to the reports of secret government surveillance of phones and Internet? And can you also assure Americans that the government — your government doesn't have some massive secret database of all their personal online information and activity?

PRESIDENT OBAMA: Yeah. You know, when I came into this office, I made two commitments that are more than any commitment I make: number one, to keep the American people safe; and number two, to uphold the Constitution. And that includes what I consider to be a constitutional right to privacy and an observance of civil liberties.

Now, the programs that have been discussed over the last couple days in the press are secret in the sense that they're classified, but they're not secret in the sense that when it comes to telephone calls, every member of Congress has been briefed on this program.

With respect to all these programs, the relevant intelligence committees are fully briefed on these programs. These are programs that have been authorized by broad, bipartisan majorities repeatedly since 2006. And so I think at the outset, it's important to understand that your duly elected representatives have been consistently informed on exactly what we're doing.

Now, let — let me take the two issues separately. When it comes to telephone calls, nobody is listening to your telephone calls. That's not what this program's about. As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls. They are not looking at people's names, and they're not looking at content. But by sifting through this so-called metadata, they may identify potential leads with respect to folks who might engage in terrorism. If these folks — if the intelligence community then actually wants to listen to a phone call, they've got to go back to a federal judge, just like they would in a criminal investigation. So I want to be very clear. Some of the hype that

we've been hearing over the last day or so — nobody's listening to the content of people's phone calls.

This program, by the way, is fully overseen not just by Congress but by the FISA Court, a court specially put together to evaluate classified programs to make sure that the executive branch, or government generally, is not abusing them and that they're — it's being out consistent with the Constitution and rule of law.

And so not only does that court authorize the initial gathering of data, but I want to repeat, if anybody in government wanted to go further than just that top-line data and wanted to, for example, listen to Jackie Calmes's phone call, they'd have to go back to a federal judge and — and — and indicate why, in fact, they were doing further — further probing.

Now, with respect to the Internet and emails, this does not apply to U.S. citizens, and it does not apply to people living in the United States. And again, in this instance, not only is Congress fully apprised of it, but what is also true is that the FISA Court has to authorize it.

So in summary, what you've got is two programs that were originally authorized by Congress, have been repeatedly authorized by Congress. Bipartisan majorities have approved (on them?). Congress is continually briefed on how these are conducted. There are a whole range of safeguards involved. And federal judges are overseeing the entire program throughout. And we're also setting up — we've also set up an audit process when I came into office to make sure that we're, after the fact, making absolutely certain that all the safeguards are being properly observed.

Now, having said all that, you'll remember when I made that speech a couple of weeks ago about the need for us to shift out of a perpetual war mindset. I specifically said that one of the things that we're going to have to discuss and debate is how were we striking this balance between the need to keep the American people safe and our concerns about privacy, because there are some trade-offs involved.

And I welcome this debate. And I think it's healthy for our democracy. I think it's a sign of maturity, because probably five years ago, six years ago, we might not have been having this debate. And I think it's interesting that there are some folks on the left, but also some folks on the right who are now worried about it who weren't very worried about it when it was a Republican president. I think that's good that we're having this discussion.

But I think it's important for everybody to understand, and I think the American people understand, that there are some trade-offs involved. You know, I came in with a health skepticism about these programs. My team evaluated them. We scrubbed them thoroughly. We actually expanded some of the oversight, increased some of the safeguards. But my assessment and my team's assessment was that they help us prevent terrorist attacks. And the modest encroachments on privacy that are involved in getting phone numbers or duration without a name attached and not looking at content — that on, you know, net, it was worth us doing.

That's — some other folks may have a different assessment of that. But I think it's important to recognize that you can't have a hundred percent security and also then have a hundred percent privacy and zero inconvenience. You know, we're going to have to make some choices as a society.

And — (audio break) — I can say is, is that in evaluating these programs, they make a difference — (audio break) — to anticipate and prevent possible terrorist activity. And the fact that they're under very

strict supervision by all three branches of government and that they do not involve listening to people's phone calls, do not involve reading the emails of U.S. citizens or U.S. residents, absent further action by a federal court, that is entirely consistent with what we would do, for example, in a criminal investigation.

I think, on balance, we — you know, we have established a process and a procedure that the American people should feel comfortable about. But again, this — these programs are subject to congressional oversight and congressional reauthorization and congressional debate. And if there are members of Congress who feel differently, then they should speak up.

And we're happy to have that debate. OK.

Q: Sir —

PRESIDENT OBAMA: All right. Then we'll have — we'll have a chance to talk further during the course of the next couple days.

Thank you, guys. Thank —

Q: Do you welcome the leak, sir? Do you welcome the leak if you welcome the debate?

PRESIDENT OBAMA: I don't — I don't welcome leaks, because there's a reason why these programs are classified. You know, I think — I think that there is a suggestion that somehow any classified program is a quote-unquote "secret" program, which means it's somehow suspicious. But the fact of the matter is, in our modern history there are a whole range of programs that have been classified because, when it comes to, for example, fighting terror, our goal is to stop folks from doing us harm, and if every step that we're taking to try to prevent a terrorist act is on the front page of the newspapers or on television, then presumably the people who are trying to do us harm are going to be able to get around our preventive measures. That's why these things are classified.

But that's also why we've set up congressional oversight. These are the folks you all vote for as your representative in Congress, and they're being fully briefed on these programs.

And if in fact there was — there were abuses taking place, presumably, those members of Congress could raise those issues very aggressively. They're empowered to do so.

We also have federal judges that we put in place who are not subject to political pressure.

They've got lifetime tenure as federal judges, and they're empowered to look over our shoulder at the executive branch to make sure that these programs aren't being abused.

So — so we have a system in which some information is classified, and we have a system of checks and balances to make sure that it's not abused. And if, in fact, this information ends up just being dumped out willy-nilly without regard to risks to the program, risks to the people involved, in some cases on other leaks, risks to personnel in very dangerous situations, then it's very hard for us to be as effective in — in protecting the American people.

That's not to suggest that, you know, you just say, trust me, we're doing the right thing, we know who the bad guys are. And the reason that's not how it works is because we've got congressional oversight and judicial oversight. And if people can't trust not only the executive branch but also don't trust Congress

and don't trust federal judges to make sure that we're abiding by the Constitution, due process and rule of law, then we're going to have some problems here.

But my observation is, is that the people who are involved in America's national security, they take this work very seriously. They cherish our Constitution. The last thing they'd be doing is taking programs like this to listen to somebody's phone calls.

And by the way, with respect to my concerns about privacy issues, I will leave this office at some point, sometime in the last — next 3 1/2 years, and after that, I will be a private citizen. And I suspect that, you know, on — on a list of people who might be targeted, you know, so that somebody could read their emails or — or listen to their phone calls, I'd probably be pretty high on that list. So it's not as if I don't have a personal interest in making sure my privacy is protected.

But I know that the people who are involved in these programs — they operate like professionals. And these things are very narrowly circumscribed. They're very focused. And in the abstract, you can complain about Big Brother and how this is a potential, you know — you know, program run amok. But when you actually look at the details, then I think we've struck the right balance.

All right? Thank you very much, guys. That's it — I — (cross talk) — thank you. (Cross talk.)

Q: (Inaudible) — are undercutting your talks with President Xi?

(No audible reply.)

Copyright 2013 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

EXHIBIT J



Ex-NSA Head Hayden: Surveillance Balances Security, Privacy

June 09, 2013 11:30 AM

Listen to the Story

Weekend Edition Sunday

8 min 14 sec

Correction

June 10, 2013

We incorrectly say it has been 13 years since the Sept. 11, 2001, attacks.

Few people know how the National Security Administration works like Gen. Michael Hayden, who once served as head of the secretive organization. Host Rachel Martin talks with Hayden about recent revelations about the agency's access to phone and electronic communications.

Copyright © 2013 NPR. For personal, noncommercial use only. See Terms of Use. For other uses, prior permission required.

RACHEL MARTIN, HOST:

This is WEEKEND EDITION from NPR News. I'm Rachel Martin.

It was a rough political week for President Obama after a string of revelations about sweeping government surveillance of American telephone records, email and Internet activity. And more fallout may come this week after further revelations in the Guardian newspaper about yet another tool that the NSA uses. It's called the Boundless Informant program and it shows that the NSA collected some 97 billion pieces of intelligence from computer networks around the world just in March of this year alone. Last night, the president's top intelligence advisor, James Clapper, criticized the latest media reports, saying they have mischaracterized the government's data

collection programs.

We are joined in the studio now by General Michael Hayden. He served as the director of the National Security Agency. He was also the director of the CIA. Thank you so much for coming in, General.

GENERAL MICHAEL HAYDEN: Yeah, thank you, Rachel.

MARTIN: President Obama and his director of national intelligence, James Clapper, have both insisted that the U.S. government is not spying on Americans.

HAYDEN: Right.

MARTIN: That it is not data-mining information from Americans.

HAYDEN: Right.

MARTIN: So, if that is the case, what is it doing? What is the purpose of this program?

HAYDEN: (Laughing) OK, so the first thing we need to keep in mind is that there are two programs here and they're getting conflated in the public coverage of what NSA is doing. So let's start with the first one.

The first one was revealed through revealing the FISA court order to Verizon. That's about metadata and it's about telephones. It's fact of call. And what happens there has been made now very clear by Director Clapper that the United States government - the National Security Agency - is acquiring as business records, not collecting on a wire anywhere, but acquiring as business records the metadata of foreign and domestic phone calls here in the United States. And that constitutes billions of events per day.

MARTIN: And this is a program that you worked on at the NSA.

HAYDEN: It is a successor to the activities we began after 9/11 on President Bush's authority, later became known as the Terrorist Surveillance Program.

So, NSA gets these records and puts them away, puts them in files. They are not touched. So, fears or accusations that the NSA then data mines or trolls through these records, they're just simply not

true.

MARTIN: Why would you be collecting this information if you didn't want to use it?

HAYDEN: Well, that's - no, we're going to use it. But we're not going to use it in the way that some people fear. You put these records, you store them, you have them. It's kind of like, I've got the haystack now. And now let's try to find the needle. And you find the needle by asking that data a question. I'm sorry to put it that way, but that's fundamentally what happens. All right. You don't troll through the data looking for patterns or anything like that. The data is set aside. And now I go into that data with a question that - a question that is based on articulable, arguable, predicate to a terrorist nexus. Sorry, long sentence.

MARTIN: You have to have just cause first.

HAYDEN: I have to have a probability as to why I'm going in there. Let me just give you a very practical and very common example. We roll up an al-Qaida cell somewhere. Let's just say Yemen. We grab a cell phone. We note through the pocket litter that the owner of that cell phone is involved in terrorist activity. We didn't know about that cell phone before. We didn't have that number. It is quite a legitimate activity then to simply - I'm being a little flip about this - walk up to the barrier of that grand database I just described for you and simply yell across the transom: Have any of you guys ever talked to this phone number?

Now, you're not touching - by the way, what happens to all the other records in that database? Absolutely nothing. You've got to have this nexus to terrorism to ask the question.

MARTIN: May I back up? Do you have to have approval...

HAYDEN: No.

MARTIN: ...from the FISA court...

HAYDEN: No.

MARTIN: ...which is the intelligence surveillance court established in order to go in and ask that question.

HAYDEN: You have had a generalized approval, and so you've got to justify the overall approach to the judge. But you do not have to go to the judge, saying, hey, I got this number now. I'll go ahead and get a FISA request written up for you. No, you don't have to do that.

MARTIN: How does the Internet surveillance program differ?

HAYDEN: OK. Separately now, go to the second program, which some people are calling PRISM, all right? Now, PRISM is about Internet data, not telephony. And it's all about foreigners. All right? Now, so, if I've got a bad person in Waziristan talking to a bad person in Yemen via a chat room that is hosted by an American Internet service provider, the only thing American about that conversation is the fact that it's happening on a server on the West Coast of the United States.

MARTIN: It's my understanding, though, that analysts who are making these determinations only have to be 51 percent sure that this person is a foreigner. That seems mushy.

HAYDEN: Yeah, well, actually, in some ways, you know, that's actually the literal definition of probable, in probable cause. And I understand. It makes Americans nervous. Fifty-one percent; you're going to get some of these wrong. But, Rachel, the way this works is you get to do the first step, based on a belief that this is probably a foreign conversation. All right? But as you go through it, you are under a constant requirement to try to shred out whether you're still sure it's foreign or American. And if it's American, you're done.

MARTIN: The NSA has been transformed by new technology, obviously, we've been talking about it, that allows for the highly automated instantaneous analysis of all of this information. Is it possible that the technology has gotten out ahead of the laws?

HAYDEN: Oh, that's always the challenge. And in fact, in fact, what we saw after 9/11, in the special authorization I got from President Bush under his Article 2 authority as commander in chief to do the Terrorist Surveillance Program, is a classic case of technology outstripping the law. I mean, the law, in this case is the FISA Act, the Foreign Intelligence Surveillance Act. It was passed in 1978. By 2001, OK, the effect of the FISA Act was inconsistent with the intent of the FISA Act. And the different effect was created by the change

in technology.

MARTIN: So, what do you do at this point? I mean, is this something that now needs to be reined in?

HAYDEN: No. No, no. Look, look. The law was changed in 2008 to reflect the change in technology. Now, what I was...

MARTIN: You think it's sufficient?

HAYDEN: Well, right now I think it's sufficient. What I was doing under the president's Article 2 authority has been made more sustainable by actually having Congress join in and actually change the law, so that you've got both political branches agreeing this is a good idea. This is an accurate reflection of balancing our security and our privacy.

MARTIN: It has been 13 years since the terrorist attacks of 9/11. We heard the president a couple of weeks ago say that he thinks that laws need to be recalibrated, that the original law, the authorization for the use of military force that legalized the war against al-Qaida perhaps needs to be looked at again. He did not mention the Patriot Act. Do you think that enough time has passed, that the war has changed enough, that that law needs to be retooled? [POST-BROADCAST CORRECTION: It has been over 11 years since the Sept. 11, 2001 attacks.]

HAYDEN: Isn't it interesting? To the degree the war is changing, it's moving in the direction of these two programs we just talked about, particularly the metadata program. I mean, we are a bit less worried about this massive, slow-moving, complex al-Qaida attack designed to create mass casualties, and we're more now worried about the one-off lone wolf, like Nazibullah Zazi or Faiza Shizad or Major Hasan.

So, in actuality, although we're safer, the tactics of our adversaries are actually moving more in the direction where we more need programs like the one we've talked about.

MARTIN: General Michael Hayden. He served as both the head of the CIA and the director of the National Security Agency. He joined us here in our studio in Washington. General Hayden, thanks so much for taking the time.

HAYDEN: Thank you.

Copyright ©2013 NPR. All rights reserved. No quotes from the materials contained herein may be used in any media without attribution to NPR. This transcript is provided for personal, noncommercial use only, pursuant to our Terms of Use. Any other use requires NPR's prior permission. Visit our permissions page for further information.

NPR transcripts are created on a rush deadline by a contractor for NPR, and accuracy and availability may vary. This text may not be in its final form and may be updated or revised in the future. Please be aware that the authoritative record of NPR's programming is the audio.

©2013 NPR

EXHIBIT K



 [Print](#)  [Close](#)

Government surveillance unconstitutional? Reaction from Sens. Rand Paul, Ron Johnson and Gen. Michael Hayden

Written by [Chris Wallace](#) [1] / Published June 09, 2013 / Fox News Sunday

Special Guests: Sen. Rand Paul, Sen. Ron Johnson, Gen. Michael Hayden

The following is a rush transcript of the June 9, 2013, edition of "Fox News Sunday With Chris Wallace." This copy may not be in its final form and may be updated.

CHRIS WALLACE, HOST: I'm Chris Wallace.

Today, are we getting closer to Big Brother?

(BEGIN VIDEOTAPE)

UNIDENTIFIED MALE: This is a big deal -- a really big deal.

WALLACE: Critics call the secret collection of millions of Americans' phone records government overreach, but others on both sides of the aisle say it's keeping us safe.

PRESIDENT BARACK OBAMA: You can't have 100 percent security and then also have 100 percent privacy and zero inconvenience.

REP. MIKE ROGERS, R-MICH.: It is legal. It's been authorized by Congress.

WALLACE: We'll talk with Senator Rand Paul who sees a pattern in the surveillance programs and the administration's scandals -- an assault on the Constitution.

And, then, we'll get an inside look at how government is looking over our shoulders from General Michael Hayden, former head of the NSA and CIA, and Senator Ron Johnson of the Homeland Security Committee.

Plus, President Obama shakes up his national security team.

OBAMA: I am extraordinarily proud to announce my new national security adviser, Susan Rice.

UNIDENTIFIED MALE: The president intentionally did not put her up for secretary of state because he did not want her facing Senate confirmation.

WALLACE: We'll ask our Sunday panel what it means for the president's second-term agenda.

All, right now, on "Fox News Sunday."

(END VIDEOTAPE)

WALLACE: And hello again from Fox News in Washington.

Revelations about the government's monitoring, phone records and emails have renewed questions about the balance between privacy and security. Combine that with the scandals involving the IRS targeting conservatives groups and the Department of Justice snooping on reporters, and critics say you have a government that's too big and too intrusive.

One of those critics is Senator Rand Paul and he joins us now from Bowling Green, Kentucky.

Senator, welcome back to "Fox News Sunday."

SEN. RAND PAUL, R-KY.: Good morning.

WALLACE: Senator, you call these government surveillance programs an astounding assault on the Constitution. President Obama calls them modest encroachments on privacy.

Take a look.

(BEGIN VIDEO CLIP)

OBAMA: In the abstract, you can complain about big brother and how this is a potential program run amok. But when you actually look at the details, then I think we've struck the right balance.

(END VIDEO CLIP)

WALLACE: Senator, in fact, all three branches of government -- the Congress, the president and the courts have all approved these surveillance programs.

How are they then unconstitutional?

PAUL: Well, you know, they're looking at a billion phone calls a day is what I read in the press and that doesn't sound to me like a modest invasion of privacy. It sounds like an extraordinary invasion of privacy. The Fourth Amendment says you can look at and ask for a warrant specific to a person, place and the items.

This is a general warrant. This is what we objected to and what our Founding Fathers partly fought the revolution over is they did not want generalized warrants where you could go from house to house with soldiers looking for things or now from computer to computer, to phone to phone, without specifying who you're targeting.

WALLACE: Let's look at the effects of the Internet surveillance program as opposed to the phone surveillance program. In 2009, we were able, the NSA was able to intercept emails between an al Qaeda bomb maker in Pakistan, Rashid Rauf, and a man in Denver, Najibullah Zazi. As a result, they were able to stop Zazi from putting backups with bombs on the New York City subway system. The program, according to the government, targets foreigners on foreign soil.

You would stop that?

PAUL: My suspicion is -- and a lot of this is classified so another side gets to promote their case and we don't get the information -- but my suspicion is that this gentleman was targeted because they suspected him for being a terrorist. I have no problem if you have probable cause and you target people who are terrorists and you go after them and people that they're communicating with, you get another warrant.

But we're talking about trolling through billions of phone records. We're not talking about going after a terrorist. I'm all for that. Get a warrant and go after a terrorist, or a murderer or a rapist. But don't troll through a billion phone records every day. That is unconstitutional, it invades our privacy and I'm going to be seeing if I can challenge this at the Supreme Court level. I'm going to be asking all the Internet providers and all of the phone companies, ask your customers to join me in a class action lawsuit. If we get 10 million Americans saying we don't want our phone records looked at then somebody will wake up and say things will change in Washington.

WALLACE: I'm going to talk about legislation in a second, but let's talk about the practical effects of this because defenders of the program say, if you want to find the needle in the haystack, you have to have the haystack first. And here's what your fellow Senator Lindsey Graham had to say about you on this issue: "In Rand Paul's world, you have almost no defenses against terrorists."

PAUL: I would say that's an unfair characterization. I want to go after terrorists as much as anyone. For example, we are looking through so much data that I think it makes our fight against terrorism worse. The Tsarnaev boy, one of the Boston marathon bombers, we didn't know that he went back to Chechnya because we're not doing enough targeted analysis. We have millions of phone calls and we can't even possibly look at all the data.

You know, we have millions of audiotape hours of people and we can't go through it. They haven't gone back through 25 percent of the audio they have. They're overwhelmed in data. So, I think it's just bad police work.

Why didn't we know the Tsarnaev boy had gone back to Chechnya? Because we're not going good police work because we're busy looking at the records of regular Americans who haven't committed any crime.

WALLACE: All right. Let's talk about your suggested remedy. You talk on the one hand about a Supreme Court challenge, but you also say that you're going to introduce something called the "Fourth Amendment Restoration Act". Now, of course, the Fourth Amendment to the Bill of Rights protects us against unreasonable searches and seizures.

So, try to get a little specific here. I know it's hard. How much would you restrict government surveillance as it now exists? And as a practical matter, do you have any reason to believe that Congress is going to go along with you on this?

PAUL: I think the American people are with me, and I think if you talk to young people who use computers on a daily basis, they're absolutely with me.

They think that your third party record -- so, for example, what I spend on my Visa each month, that's my business and where I spend it and whether I read conservative magazines, whether I subscribe to FOX News, or whether I subscribe to Yahoo or Google.

What I do in my private life is my private life. If you suspect me of a crime, have probable cause.

Over the last 30 or 40 years, we've said, once you give your records to your bank or your Visa company, that they're no longer private. I disagree vehemently with that. That is, of course, we have to reverse because so much of our life now is digitalized that we have to protect it from a snooping government.

And we've now got a government that appears to target people based on our political beliefs. So, I don't want my records given to an administration that I can't trust.

WALLACE: All of this -- well, let's pick up on that, because all of this comes at a time when President Obama is involved in scandals or his administration is, the IRS targeting conservatives, the Department of Justice snooping on reporters.

Do you see a pattern? Do you see a connection between the scandals and these government surveillance programs?

PAUL: Yes, because I think it really makes people distrust their government even more, when they're seeing the IRS being used after political opponent. But this much power is too much power to give any government. I don't care if it's a Republican government or Democratic government, I don't want that much power given to a president and I think it's very worrisome.

And I think if the young people in this country wake up and say, "Enough's enough and we don't want them looking at our phone records," I think we could reverse this. When we went after the SOPA and PIPA legislation that we thought was going to invade the due process of the Internet, people by the millions came out.

If we can have that again -- people by the millions coming out and saying, "Look, I want to be part of a class action suit that says to the government, let's hear this at the Supreme Court level. Are you allowed to look at phone records even though there's no probable cause that I'm related to a crime?" -- I think we'll put an end to this.

WALLACE: I want to turn to foreign policy. This week, the president named Susan Rice, the former U.N. ambassador to be the new national security adviser to the president in the White House. You say, instead of being promoted, he should have fired her from misleading the country on Benghazi. The problem, of course, from your point of view is, she's not subject to Senate confirmation.

But, as a member of the Senate Foreign Relations Committee, will you use two others -- former State Department spokeswoman Victoria Nuland and Samantha Power who has been named as U.N. ambassador -- will you use their nominations and the committee to demand answers on Benghazi?

PAUL: I think both Ms. Nuland, as well as Ambassador Rice, were intimately involved with a misleading campaign or a misdirection campaign after Benghazi. And I think really you shouldn't promote someone who has been misleading -- purposely misleading the American public.

No, I think it's appalling. And so, I think neither one should be to their position. I don't have the possibility of stopping Ambassador Rice. Ms. Nuland, we're going to look at because she was Hillary Clinton's spokesman who says she had nothing to talking points, even though her spokesman was rewriting them all night long to try to get out any references to terrorism.

I still don't think we've gotten to the bottom of why they had this elaborate misdirection campaign when obviously everybody thought it was a terrorist attack from the beginning.

So, it really wasn't designed to work unless, really, the misdirection campaign was to get us away from the fact that the CIA annex there was dealing in arms to Syria through Turkey, which was illegal at the time.

WALLACE: So, just to follow up, are you going demand answers in Benghazi in the Nuland confirmation hearing? And would you, conceivably, as part of that, put a hold on her nomination?

PAUL: I haven't made a decision on the Nuland nomination yet. But we are going look very carefully and I will be asking probing questions because I still want to know why we were misdirected, why was Ms. Nuland involved? And did she talk to Hillary Clinton that night.

I would never have my press spokesman making statements for me throughout the night on an international crisis without talking to me. So, Hillary Clinton says, "Oh, I had nothing to do with the talking points." Well, her spokesman all night long was rewriting the talking points -- I just find it beyond credulity.

WALLACE: Let me turn to another subject. On Friday, the Senate began debate on comprehensive immigration reform. You say you support that idea in concept.

On the other hand, you now have come out against a new path to citizenship and you say that before any reform that the border has to be secured first.

Senator, as a practical matter, isn't that going to prevent any kind of comprehensive reform?

PAUL: No. I still think we can have immigration reform. I think we need to fix the system. The reason why we have 11 million undocumented people here is because we have a broken visa system. About half of them came here to work legally, but then they found a better-paying job and we prevent them from being -- going from a farm job to a construction job.

Guess what? This bill does the same thing.

So, if you don't fix that problem, you don't fix why we have illegal immigration. You need to expand the numbers of workers that are allowed to come to this country. That means I'm all for immigration, but this bill actually puts new caps on immigrants coming out here to pick crops.

So, it does some of the wrong things, and then it doesn't secure the border. It says to the administration -- hey, guys why don't you have a plan to build a fence that we authorized 10 years ago?

I think that's absurd and that's like Obamacare, oh, here, you, the administration, you guys do it. Instead of Congress doing their job and just writing the bill saying, my amendment will say you have to build 100 miles of fence each year and Congress votes on whether or not the border is secure.

(CROSSTALK)

PAUL: I think that's the only way to guarantee they're secure.

WALLACE: But just briefly, Senator, you know, you got to tradeoff here. You've got Democrats who want to get citizenship for the 11 million illegals who are here. You've got Republicans who want tougher border enforcement. If you're not willing to compromise on those, you don't get comprehensive reform.

PAUL: I am willing to compromise.

For example, I would let you, if you have a work visa also stand in the citizenship line, but not a new citizenship line. There current exist a line that if you're in Mexico City right now and you want to come and be a citizen in our country, you get in that line. I would let workers who are here on work visa get in the same line, but I wouldn't create a new pathway or a new line.

What happens is, is right now, it's illegal to stand in both lines. If you're here on a work visa, you're not allowed to stand in line to come into the country permanently. I would let you stand in both lines which would be a legal change, but I wouldn't create a new pathway.

The whole point is, there needs to be a conduit. I am the conduit between conservatives in the House who don't want these things and more moderate people in the Senate who do want these things. I want to make the bill work, but see, the thing is, is what they have in the Senate has zero chance of passing in the House. So, why not come to a conservative like myself and say, he's willing to work with you, why not work with me to make the bill closer to what would be acceptable in the House?

So, I'm really trying to make immigration work. But they're going to have to come to me and they're going have to work with me to make the bill stronger if they want me to vote for it.

WALLACE: We're going to stay on top of it. Senator Paul, thank you so much for coming in today, sir.

PAUL: Thank you.

WALLACE: Up next, the president pushes back over accusations his administration is spying on Americans.

(BEGIN VIDEO CLIP)

OBAMA: Nobody's listening to the content of people's phone calls.

(END VIDEO CLIP)

WALLACE: We'll continue our discussion of government surveillance with a man who used to do it for a living.

(COMMERCIAL BREAK)

WALLACE: Senator Paul has painted a picture of unconstitutional government overreach.

We want to hear now from fellow Republican, Senator Ron Johnson, who joins us from Green Bay, Wisconsin.

And here in Washington, General Michael Hayden, former head of the NSA and the CIA, who used to run the government surveillance programs. He's now a global security consultant.

Senator Johnson, you just heard Rand Paul. Do you think that we need more restriction on these government surveillance programs?

SEN. RON JOHNSON, R-WIS.: Good morning, Chris.

Listen, I'm every bit as concerned about civil liberties as Senator Paul and quite honestly -- quite honestly, as most persons are, and that's a good thing. You know, this is not a partisan issue. Across the political spectrum, people are concerned about preserving our liberties and maintaining our civil liberties.

But, at the same time, you know, we have -- we face a very real, asymmetric threat in international terrorism, and our greatest line of defense against that terrorism is intelligence-gathering capabilities.

And so, we have to maintain that and it is a very delicate balance and that balance shifts based on circumstances, and based on the time. But, you know, we do need congressional oversight on this. It's a good thing that these laws come up for reauthorization.

So, I'm every bit as concerned with civil liberties and then we're going to be conducting robots to oversight on these -- on these programs.

WALLACE: General Hayden, let's talk first of all about the general reaction you have to Senator Paul. I'm going to get into specific issues with you. As a man who used to run these programs, how important and how effective have they been in keeping us safe and how do you feel when you hear Senator Paul talk about class action lawsuits to the Supreme Court, new congressional restrictions?

GEN. MICHAEL HAYDEN, FORMER HEAD OF NSA AND CIA: Well, first of all, Chris, with regard to how effective they are, I think they're very effective. We had two presidents doing the same thing with regard to electronic surveillance. Now, that seems to me to suggest that these things do work.

Now, with regard to what the senator said -- if I believed NSA was doing some of the things the senator fears

they're doing, I would have been backstopping him during your first segment. He said we're trolling through millions of records. That's just simply not true.

The government acquires records as business records from the telecom providers, but then doesn't go into that database without an arguable reason connected to terrorism to ask that database a question. If you don't have any link to that original predicate, terrorism, your phone records are never touched.

WALLACE: Well, let's get into that and let's talk a little bit -- and I know we're getting into kind of a sensitive area here about the tradecraft that you were involved with -- as especially the head of the NSA, but also the CIA.

According to one estimate, the NSA is getting the phone records of 3 billion of our phone calls every day -- 3 billion phone calls every day.

Two questions: one, how can you possibly process 3 billion records a day? And, secondly, why not just target, from the very beginning, the bad guys?

HAYDEN: Well -- well, first of all, you have to identify who are the bad guys. So, let's begin the acquisition. Three billions is a big number.

Keep in mind, Chris, that our telecommunications providers do that every day on their own. So, it's not impossible to do. Now you've got the data stored.

Here's the important part and this is the part that protects civil liberties and balances, which Senator Johnson wants to balance -- security and our freedom.

You ask the database a question, but the question has to be related to terrorism. I'll give you a concrete example so this is very clear. So, you roll up something in Waziristan. You get a cell phone. It's the first time you've ever had that cell phone number. You know it's related to terrorism because of the pocket litter you've gotten in that operation.

Here's how it works: you simply ask that database, hey, any of you phone numbers in there ever talked to this phone number in Waziristan? I mean, you're already going into the database with the predicate, with a probable cause, with an arguable reason why you're asking for the data.

WALLACE: I've been talking -- obviously, this has been the subject in Washington and across the country this week. People are concerned about this mountain of data that you have.

OK. I mean, what you say sounds perfectly sensible. You know that there's a guy in Waziristan. You want to know who he's talking to in the United States.

One, what do you do with all the records, the billions of records that you have on all of us law-abiding citizens and what's the potential for abuse with the fact that you have all of that stored in computers somewhere?

HAYDEN: First, to answer your question, what do we do with all of the other records? Nothing. All right?

WALLACE: You keep it, though.

HAYDEN: Of course, because -- I mean, you get the cell phone with that number six months from now you want to know the history of that number. When does the value of that information begin to age off?

So, you do retain the information so that you can ask questions of it in the future. With regard to abuse, there are no records of abuse under President Bush, under President Obama.

Now, I was criticized because I theoretically didn't have enough oversight mechanisms, but no one accused us of abuse. President Obama has in some ways added incredible oversight mechanisms to this. Again, no abuse under either president.

WALLACE: Let me ask you about Obama and I promise, Senator Johnson, I'm going to bring you back in after this final question. Back in 2006, Senator Obama voted against your nomination to be CIA director because of your involvement in government programs,

From what you know and I understand you've been on the outside, how much has he changed? He expanded, restricted these government surveillance programs that he inherited.

HAYDEN: In terms of surveillance?

WALLACE: Yes.

HAYDEN: Expanded in volume, changed the legal grounding for them a little bit, put it more under congressional authorization rather than the president's Article II powers and added a bit more oversight.

But in terms of what NSA is doing, there is incredible continuity between the two presidents.

WALLACE: How do you mean he's expanded in volume?

HAYDEN: Well, it may just because we've gotten more of these records over time and with the amendment to the FISA Act in 2008, which Senator Obama finally voted for, NSA is actually empowered to do more things than I was empowered to do under President Bush's special authorization.

WALLACE: Let's turn to foreign policy. Senator Johnson, as we discussed with Senator Paul, the president named a new national security adviser this week, Susan Rice, the former U.N. ambassador who infamously went out on the Sunday talk shows.

One, what do you think of that? And two, I'm going to ask you the same question I asked of Senator Paul. You are also a member of the Senate Foreign Relations. What do you think about the nominations of Victoria Nuland, who was Hillary Clinton's spokeswoman during Benghazi, as an assistant secretary of state, and Samantha power as U.N. ambassador? And will you use their nominations to try to get answers on Benghazi?

JOHNSON: Well, first of all, Chris, it's not surprising that President Obama appointed Secretary Rice. But it's disappointing that he's chosen this moment when -- let's face it -- his administration is going through a crisis of credibility.

The reason this NSA thing has blown up is because the American people have lost their faith in President Obama and his administration. I mean, I'm not the only one saying that. "The New York Times" is saying this administration has lost all credibility.

And so, Susan Rice was the person at the center of misleading America on Benghazi and so it's incredibly disappointing. And what we need to do on Benghazi, the next step is we need to get the names of the survivors and we need to get those folks up in front of Congress and to tell us exactly what happened and what assets might have been in place.

So, if we have to utilize some of these nominations to get that information I think that might be an appropriate course of action.

WALLACE: Would you --

JOHNSON: But Americans are just losing faith in this administration and that's not a good thing.

WALLACE: Would you consider putting a hold on either the Nuland or Power nominations to -- as leverage to get this information?

JOHNSON: I think that's a possibility.

You know, when Secretary Clinton came before our committee in response to my questioning her, she asked her own question, what difference does it make? We're starting to see the difference it makes when the American people lose faith in this administration.

But, you know, I think a healthy mistrust of government is a good thing, but what I look to do is make sure the Americans start taking a look at the awesome power of government in other areas, you know, the ability to take 45 percent of your income, 40 percent of your estate, tell you what doctor to utilize, you know, what type of health treatments are going to be made available to you.

So, this is about limiting our government and Americans do need to be very skeptical of an ever-expanding, ever-more-powerful government.

WALLACE: General Hayden, I want on to ask you about another aspect of the Benghazi attack because you would have a first hand from your experience and that's the talking point and the whole process involving the talking points.

I want to put up on the screen, the first draft you see on the left those were the first talking points drafted by the CIA. They talked about links to al Qaeda, about months of attacks against Western interest in Benghazi before the fatal attack on the U.S. consulate. All of that was taken out of the much smaller talking points you see there on the right that Susan Rice used on the Sunday talk shows.

This, obviously, is much more publicized than usually it is. From what you've read, is it -- is there anything unusual about the editing process in this case?

HAYDEN: Oh, the most unusual, Chris, is that CIA was writing the talking points.

Look, on a good Sunday morning on the talk shows, you get policy talk. On most Sunday mornings you get political talk. Neither of those are intelligence talk. So, why is the intelligence organization writing when the page is blank?

The way this should happen, Chris, is it's a policy guise. Right now, what it is they want to reveal to the American people and they send it up river for the CIA -- not to be flip here -- to check the spelling and the facts.

Look, al Qaeda, terrorist, extremist -- those are all words that we use to accurately describe what happened there. But each one of them is freighted with political cargo. Why do you put the intelligence organization in the role of deciding which of those words to use?

WALLACE: As it turned out, they didn't decide. It was decided by the policy and political people.

How do you explain what was left out?

HAYDEN: I explained it through a very bad process that began bad by having the intelligence guys draw up the first points.

WALLACE: Finally, Senator Johnson --

JOHNSON: Chris, can I just quick --

WALLACE: Yes, sure. Go ahead.

JOHNSON: OK. I think what this administration was trying to really cover up was really their gross negligence, really, the fact that they did not -- not only provide the security that was necessary in Benghazi, but they actually denied -- they actually rammed down the security, basically made the American people believe that all was well in Benghazi, all was well with their policies leading from behind, and that's the real story behind Benghazi and that's where we need to get the bottom of. **WALLACE:** I've got less than a minute left. Senator Johnson, very generally and briefly, on immigration -- which is now on the Senator floor, the big issue on the senate floor. What changes do you need to see in the legislation for you to support it?

JOHNSON: Well, I want to see an immigration bill passed because we have to fix this system. It's not good for anybody. We definitely need to make sure that the borders are going to be secure, and we also need to make sure that, you know, basically, benefits don't flow to people that are here illegally.

And so, really, I'm very hopeful that we can pass a bill. But I agree with Senator Paul, the challenge is getting it to the House. So we're going to have to strengthen those provisions in the Senate, so we have a bill that passes the House. It doesn't do anybody any good just to pass in the Senate.

WALLACE: Senator Johnson, General Hayden, I want to talk you both for coming in today.

HAYDEN: Thank you.

WALLACE: Pleasure to talk with you as always.

JOHNSON: Have a great day.

WALLACE: Is the government's monitoring of phone calls and the Internet over the line or the new normal? Our Sunday panel joins the debate, next.

(COMMERCIAL BREAK)

(BEGIN VIDEO CLIP)

OBAMA: As for our common defense, we reject as false the choice between our safety and our ideals.

We're going to have to make some choices.

(END VIDEO CLIP)

WALLACE: President Obama's message on privacy versus security seems to have changed since his first inauguration in 2009. Time now to bring in our Sunday group: Bill Kristol of The Weekly Standard; Mara Liasson from National Public Radio; Republican strategist Mary Matalin and Peter Baker of The New York Times.

Well, Bill, as someone who I suspect thinks that these surveillance programs are a necessary part of the war on terror, do you worry that all the leaks, all the disclosures this week are going to create some sort of backlash?

BILL KRISTOL, THE WEEKLY STANDARD: I do, particularly because they're coming into context of genuine abuses of government power, especially by the IRS.

I think the big thing to remember is national security is different from internal management of the

EXHIBIT L

Wyden Statement Responding to Director Clapper's Statements About Collection on Americans

Tuesday, June 11, 2013

Washington, D.C. – U.S. Senator Ron Wyden (D-Ore.) issued the following statement regarding [statements](#) made by the Director of National Intelligence James Clapper about collection on Americans. Wyden is a senior member of the Senate Intelligence Committee.

“One of the most important responsibilities a Senator has is oversight of the intelligence community. This job cannot be done responsibly if Senators aren’t getting straight answers to direct questions. When NSA Director Alexander failed to clarify previous public statements about domestic surveillance, it was necessary to put the question to the Director of National Intelligence. So that he would be prepared to answer, I sent the question to Director Clapper’s office a day in advance. After the hearing was over my staff and I gave his office a chance to amend his answer. Now public hearings are needed to address the recent disclosures and the American people have the right to expect straight answers from the intelligence leadership to the questions asked by their representatives.”



Ron Wyden
@RonWyden

Follow

Strong congressional oversight means asking direct questions & getting straight answers.

1.usa.gov/1aoEIY3

7:13 AM - 11 Jun 2013

[Wyden Statement Responding to Director Clapper's Statements About...](#)

Washington, D.C. U.S. Senator Ron Wyden (D-Ore.) issued the following statement regarding statements made by the Directo



Ron Wyden @RonWyden

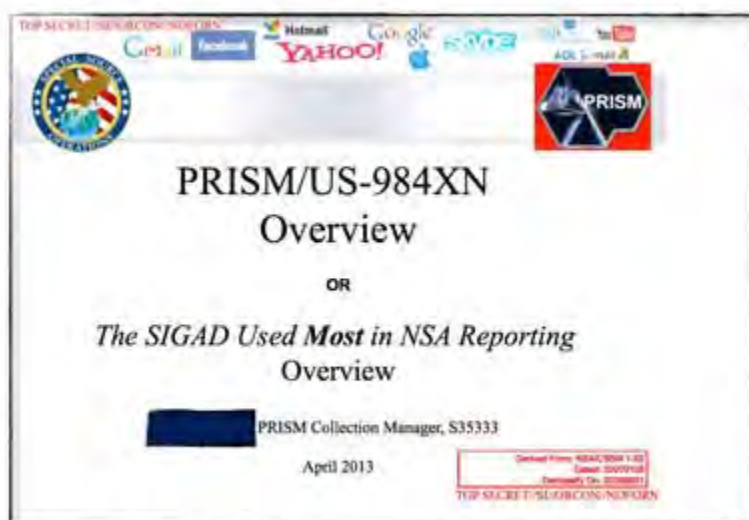
74 RETWEETS 24 FAVORITES

EXHIBIT M

NSA Prism program taps in to user data of Apple, Google and others

- Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook
- Companies deny any knowledge of program in operation since 2007
- Obama orders US to draw up overseas target list for cyber-attacks

Glenn Greenwald and Ewen MacAskill
The Guardian, Thursday 6 June 2013



A slide depicting the top-secret PRISM program.

The National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the Guardian.

The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says.

The Guardian has verified the authenticity of the document, a 41-slide PowerPoint presentation – classified as top secret with no distribution to foreign allies – which was apparently used to train intelligence operatives on the capabilities of the program. The document claims "collection directly from the servers" of major US service providers.

Although the presentation claims the program is run with the assistance of the companies, all those who responded to a Guardian request for comment on Thursday denied knowledge of any such program.

In a statement, Google said: "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a back door for the government to access private user data."

Several senior tech executives insisted that they had no knowledge of Prism or of any similar scheme. They said they would never have been involved in such a program. "If they are doing this, they are doing it without our knowledge," one said.

An Apple spokesman said it had "never heard" of Prism.

The NSA access was enabled by changes to US surveillance law introduced under President Bush and renewed under Obama in December 2012.



The program facilitates extensive, in-depth surveillance on live communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

It also opens the possibility of communications made entirely within the US being collected without warrants.

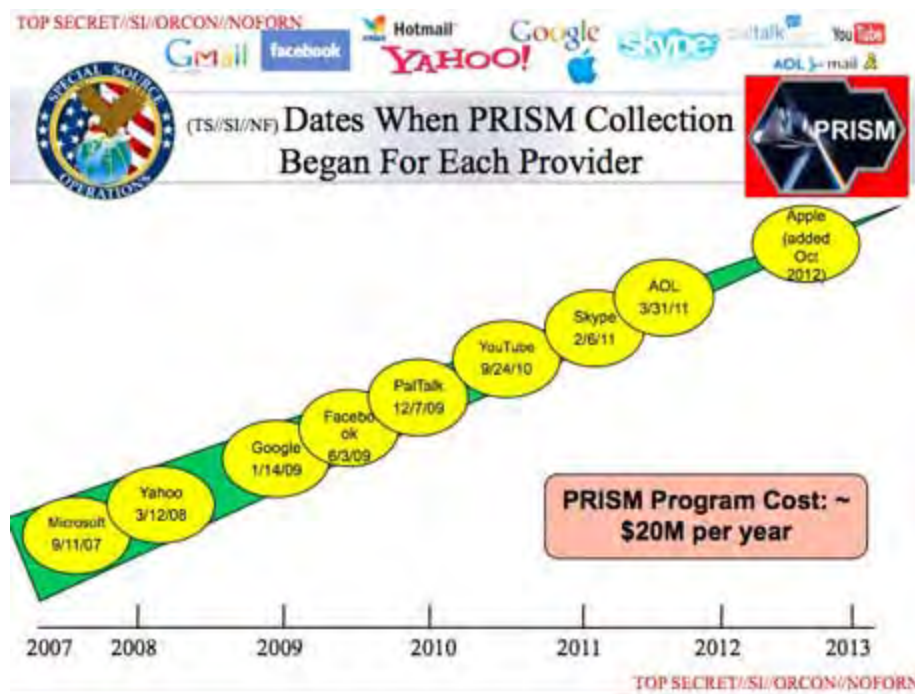
Disclosure of the Prism program follows a leak to the Guardian on Wednesday of a top-secret court order compelling telecoms provider Verizon to turn over the telephone records of millions of US customers.

The participation of the internet companies in Prism will add to the debate, ignited by the Verizon revelation, about the scale of surveillance by the intelligence services. Unlike the collection of those call records, this surveillance can include the content of communications and not just the metadata.

Some of the world's largest internet brands are claimed to be part of the information-sharing program since its introduction in 2007. Microsoft – which is currently running an advertising campaign with the slogan "Your privacy is our priority" – was the first, with collection beginning in December 2007.

It was followed by Yahoo in 2008; Google, Facebook and PalTalk in 2009; YouTube in 2010; Skype and AOL in 2011; and finally Apple, which joined the program in 2012. The program is continuing to expand, with other providers due to come online.

Collectively, the companies cover the vast majority of online email, search, video and communications networks.



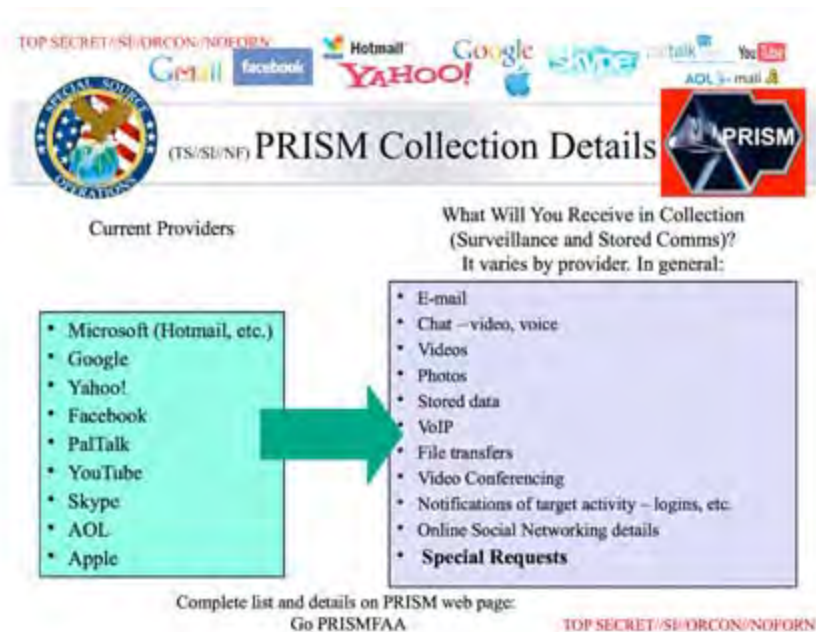
The extent and nature of the data collected from each company varies.

Companies are legally obliged to comply with requests for users' communications under US law, but the Prism program allows the intelligence services direct access to the companies' servers. The NSA document notes the operations have "assistance of communications providers in the US".

The revelation also supports concerns raised by several US senators during the renewal of the Fisa Amendments Act in December 2012, who warned about the scale of surveillance the law might enable, and shortcomings in the safeguards it introduces.

When the FAA was first enacted, defenders of the statute argued that a significant check on abuse would be the NSA's inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the Prism program renders that consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies' servers.

A chart prepared by the NSA, contained within the top-secret document obtained by the Guardian, underscores the breadth of the data it is able to obtain: email, video and voice chat, videos, photos, voice-over-IP (Skype, for example) chats, file transfers, social networking details, and more.



The document is recent, dating to April 2013. Such a leak is extremely rare in the history of the NSA, which prides itself on maintaining a high level of secrecy.

The Prism program allows the NSA, the world's largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.

With this program, the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users.

The presentation claims Prism was introduced to overcome what the NSA regarded as

shortcomings of Fisa warrants in tracking suspected foreign terrorists. It noted that the US has a "home-field advantage" due to housing much of the internet's architecture. But the presentation claimed "Fisa constraints restricted our home-field advantage" because Fisa required individual warrants and confirmations that both the sender and receiver of a communication were outside the US.

"Fisa was broken because it provided privacy protections to people who were not entitled to them," the presentation claimed. "It took a Fisa court order to collect on foreigners overseas who were communicating with other foreigners overseas simply because the government was collecting off a wire in the United States. There were too many email accounts to be practical to seek Fisas for all."

The new measures introduced in the FAA redefines "electronic surveillance" to exclude anyone "reasonably believed" to be outside the USA – a technical change which reduces the bar to initiating surveillance.

The act also gives the director of national intelligence and the attorney general power to permit obtaining intelligence information, and indemnifies internet companies against any actions arising as a result of co-operating with authorities' requests.

In short, where previously the NSA needed individual authorisations, and confirmation that all parties were outside the USA, they now need only reasonable suspicion that one of the parties was outside the country at the time of the records were collected by the NSA.

The document also shows the FBI acts as an intermediary between other agencies and the tech companies, and stresses its reliance on the participation of US internet firms, claiming "access is 100% dependent on ISP provisioning".

In the document, the NSA hails the Prism program as "one of the most valuable, unique and productive accesses for NSA".

It boasts of what it calls "strong growth" in its use of the Prism program to obtain communications. The document highlights the number of obtained communications increased in 2012 by 248% for Skype – leading the notes to remark there was "exponential growth in Skype reporting; looks like the word is getting out about our capability against Skype". There was also a 131% increase in requests for Facebook data, and 63% for Google.

The NSA document indicates that it is planning to add Dropbox as a PRISM provider. The agency also seeks, in its words, to "expand collection services from existing providers".

The revelations echo fears raised on the Senate floor last year during the expedited

debate on the renewal of the FAA powers which underpin the PRISM program, which occurred just days before the act expired.

Senator Christopher Coons of Delaware specifically warned that the secrecy surrounding the various surveillance programs meant there was no way to know if safeguards within the act were working.

"The problem is: we here in the Senate and the citizens we represent don't know how well any of these safeguards actually work," he said.

"The law doesn't forbid purely domestic information from being collected. We know that at least one Fisa court has ruled that the surveillance program violated the law. Why? Those who know can't say and average Americans can't know."

Other senators also raised concerns. Senator Ron Wyden of Oregon attempted, without success, to find out any information on how many phone calls or emails had been intercepted under the program.

When the law was enacted, defenders of the FAA argued that a significant check on abuse would be the NSA's inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the Prism program renders that consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies' servers.

When the NSA reviews a communication it believes merits further investigation, it issues what it calls a "report". According to the NSA, "over 2,000 Prism-based reports" are now issued every month. There were 24,005 in 2012, a 27% increase on the previous year.

In total, more than 77,000 intelligence reports have cited the PRISM program.

Jameel Jaffer, director of the ACLU's Center for Democracy, that it was astonishing the NSA would even ask technology companies to grant direct access to user data.

"It's shocking enough just that the NSA is asking companies to do this," he said. "The NSA is part of the military. The military has been granted unprecedented access to civilian communications.

"This is unprecedented militarisation of domestic communications infrastructure. That's profoundly troubling to anyone who is concerned about that separation."

A senior administration official said in a statement: "The Guardian and Washington Post articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act. This law does not allow the targeting of any US citizen or of any person located within the United States.

"The program is subject to oversight by the Foreign Intelligence Surveillance Court, the Executive Branch, and Congress. It involves extensive procedures, specifically approved by the court, to ensure that only non-US persons outside the US are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about US persons.

"This program was recently reauthorized by Congress after extensive hearings and debate.

"Information collected under this program is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats.

"The Government may only use Section 702 to acquire foreign intelligence information, which is specifically, and narrowly, defined in the Foreign Intelligence Surveillance Act. This requirement applies across the board, regardless of the nationality of the target."

Additional reporting by James Ball and Dominic Rushe



Get the Guardian's daily US email

Our editors' picks for the day's top news and commentary delivered to your inbox each morning.

[Sign up for the daily email](#)

More from the Guardian [What's this?](#)

[Anger swells after NSA phone records court order revelations](#) 06 Jun 2013

[Clapper admits secret NSA surveillance program to access user data](#) 07 Jun 2013

[PRISM scandal: tech giants flatly deny allowing NSA direct access to servers](#) 07 Jun 2013

[Obama's Verizon surveillance reveals massive erosion of US civil liberties](#) 06 Jun 2013

[On whistleblowers and government threats of investigation](#) 07 Jun 2013

More from around the [What's this?](#)

web

[Ford thrilled with new hybrid's performance](#) (Ford)

[Kristin Chenoweth's Incredible 88-Pound Bikini Body Is a Must-See](#) (CafeMom)

[The Surprising Relationship Between Big Data and Healthcare](#) (Intel)

[The #1 Network Security Myth](#) (Windstream Business Blog)

[United Airlines Sued By Teen For Failing to Stop Lewd Passenger](#) (Yahoo!)

EXHIBIT N

The Washington Post

[Back to previous page](#)

U.S., company officials: Internet surveillance does not indiscriminately mine data

By [Robert O'Harrow Jr.](#), [Ellen Nakashima](#) and
[Barton Gellman](#), Published: June 8



The director of national intelligence on Saturday stepped up his public defense of a top-secret government [data surveillance program](#) as technology companies began privately explaining the mechanics of its use.

The program, [code-named PRISM](#), has enabled national security officials to collect e-mail, videos, documents and other material from at least nine U.S. companies over six years, including Google, Microsoft and Apple, according to documents obtained by The Washington Post.

The disclosures about PRISM have renewed a national debate about the surveillance systems that sprang up after the attacks of Sept. 11, 2001, how broad those systems might be and the extent of their reach into American lives.

In a statement issued Saturday, Director of National Intelligence James R. Clapper Jr. described PRISM as “an internal government computer system used to facilitate the government’s statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision.”

“PRISM is not an undisclosed collection or data mining program,” the statement said.

Clapper also said that “the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence.”

The statement from Clapper is both an affirmation of PRISM and the government’s strongest defense of it since its disclosure by The Post and the Guardian on Thursday. On Wednesday, the Guardian also disclosed secret orders enabling the [National Security Agency](#) to obtain data from [Verizon](#) about millions of phone calls made from the United States.

Clapper called the disclosures “rushed” and “reckless,” with “inaccuracies” that have left “significant misimpressions.”

“Disclosing information about the specific methods the government uses to collect communications can obviously give our enemies a ‘playbook’ of how to avoid detection,” Clapper said. “Nonetheless, [the law

governing PRISM] has proven vital to keeping the nation and our allies safe. It continues to be one of our most important tools for the protection of the nation's security.”

In responding to the revelations about PRISM, the White House, some lawmakers and company officials have repeatedly suggested that secret court orders are issued every time the NSA or other intelligence agencies seek information under Section 702 of the Foreign Intelligence Surveillance Act. But the orders, which are also secret, serve as one-time blanket approvals for data acquisition and surveillance on selected foreign targets for periods of as long as a year.

The companies have publicly denied any knowledge of PRISM or any system that allows the government to directly query their central servers. But because the program is so highly classified, only a few people at most at each company would legally be allowed to know about PRISM, let alone the details of its operations.

Executives at some of the participating companies, who spoke on the condition of anonymity, acknowledged the system's existence and said it was used to share information about foreign customers with the NSA and other parts of the nation's intelligence community.

These executives said PRISM was created after much negotiation with federal authorities, who had pressed for easier access to data they were entitled to under previous orders granted by the secret FISA court.

One top-secret document obtained by The Post described it as “Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.”

Intelligence community sources said that this description, although inaccurate from a technical perspective, matches the experience of analysts at the NSA. From their workstations anywhere in the world, government employees cleared for PRISM access may “task” the system and receive results from an Internet company without further interaction with the company's staff.

In intelligence parlance, PRISM is the code name for a “signals intelligence address,” or SIGAD, in this case US-984XN, according to the NSA's official classified description of PRISM and sources interviewed by The Post. The SIGAD is used to designate a source of electronic information, a point of access for the NSA and a method of extraction. In those terms, PRISM is not a computer system but a set of technologies and operations for collecting intelligence from Facebook, Google and other large Internet companies.

According to a more precise description contained in a classified NSA inspector general's report, also obtained by The Post, PRISM allows “collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations,” rather than directly to company servers. The companies cannot see the queries that are sent from the NSA to the systems installed on their premises, according to sources familiar with the PRISM process.

Crucial aspects about the mechanisms of data transfer remain publicly unknown. Several industry officials told The Post that the system pushes requested data from company servers to classified computers at FBI facilities at Quantico. The information is then shared with the NSA or other authorized intelligence agencies.

According to slides describing the mechanics of the system, PRISM works as follows: NSA employees engage the system by typing queries from their desks. For queries involving stored communications, the queries pass first through the FBI's electronic communications surveillance unit, which reviews the search terms to ensure there are no U.S. citizens named as targets.

That unit then sends the query to the FBI's data intercept technology unit, which connects to equipment at the Internet company and passes the results to the NSA.

The system is most often used for e-mails, but it handles chat, video, images, documents and other files as

well.

“The server is controlled by the FBI,” an official with one of the companies said. “We do not offer a download feature from our server.”

Another industry official said, “No one wants the bureau logging into the company server.”

On Friday, President Obama defended the secret surveillance program, saying it makes “a difference in our capacity to anticipate and prevent possible terrorist activity.”

Obama said Congress was fully informed about the efforts, which are tightly controlled by legal authorities under FISA. “If every step that we’re taking to try to prevent a terrorist act is on the front page of the newspapers or on television,” he said, “then presumably the people who are trying to do us harm are going to be able to get around our preventive measures.”

Clapper’s statement Saturday emphasized that the program was legal under Section 702 of FISA, as approved by Congress in 2008.

The law governs surveillance of foreign nationals. It was originally passed in 1978, after scandals involving the FBI, IRS and White House during the civil rights movement of the 1960s and the Vietnam War.

Section 702 provides the post-911 legal framework for the “targeted acquisition” of intelligence about foreign persons outside the United States. The information can be obtained only under a FISA court order and a written directive from the attorney general and the director of national intelligence.

Under Section 702, the attorney general and director of national intelligence must show the FISA court that they have procedures “reasonably designed to ensure” that their intercepts will target foreigners “reasonably believed” to be overseas.

“Service providers supply information to the Government when they are lawfully required to do so,” Clapper said Saturday.

The law prohibits officials from intentionally targeting data collection efforts at U.S. citizens or anyone in the United States. The standards for intentional targeting require that an analyst have a “reasonable belief,” at least 51 percent confidence, that the target is a foreign national.

The law also provides “an extensive oversight regime, incorporating reviews by the Executive, Legislative and Judicial branches,” Clapper said in the statement.

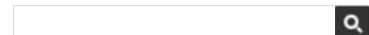
One top-secret document shows that the government is making systematic use of PRISM. An internal presentation of 41 briefing slides on PRISM suggested the scale of data collection. It described the system as the most prolific contributor to the President’s Daily Brief, which cited PRISM data in 1,477 items last year. According to the slides and other supporting materials obtained by The Post, “NSA reporting increasingly relies on PRISM” as its leading source of raw material, accounting for nearly one in seven intelligence reports.

Craig Timberg contributed to this report.

EXHIBIT O

POLITICS

In the News | Spurs-Heat | Trent Franks | Edward Snowden | Lung transplant | Colo. wildfires



More

NSA slides explain the PRISM data-collection program

Published: June 6, 2013

Through a top-secret program authorized by federal judges working under the Foreign Intelligence Surveillance Act (FISA), the U.S. intelligence community can gain access to the servers of nine Internet companies for a wide range of digital data. Documents describing the previously undisclosed program, obtained by The Washington Post, show the breadth of U.S. electronic surveillance capabilities in the wake of a widely publicized controversy over warrantless wiretapping of U.S. domestic telephone communications in 2005. These slides, annotated by The Washington Post, represent a selection from the overall document, and certain portions are redacted. [Read related article.](#)

Introducing the program

A slide briefing analysts at the National Security Agency about the program touts its effectiveness and features the logos of the companies involved.

The seal of Special Source Operations, the NSA term for alliances with trusted U.S. companies.



The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables.

PRISM/US-984XN Overview

OR

The SIGAD Used Most in NSA Reporting Overview

This note indicates that the program is the number one source of raw intelligence used for NSA analytic reports.



April 2013

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901
TOP SECRET//SI//ORCON//NOFORN

Monitoring a target's communication

This diagram shows how the bulk of the world's electronic communications move through companies based in the United States.

TOP SECRET//SI//ORCON//NOFORN

Gmail facebook msn Hotmail! Google Apple skype paltalk.com YouTube AOL mail

(TS//SI//NF) **Introduction**

U.S. as World's Telecommunications Backbone




- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011
Source: Telegeography Research
TOP SECRET//SI//ORCON//NOFORN

Providers and data

The PRISM program collects a wide range of data from the nine companies, although the details vary by provider.

TOP SECRET//SI//ORCON//NOFORN

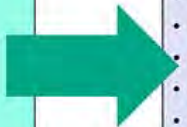
Gmail facebook msn Hotmail! Google Apple skype paltalk.com YouTube AOL mail

(TS//SI//NF) **PRISM Collection Details**




Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

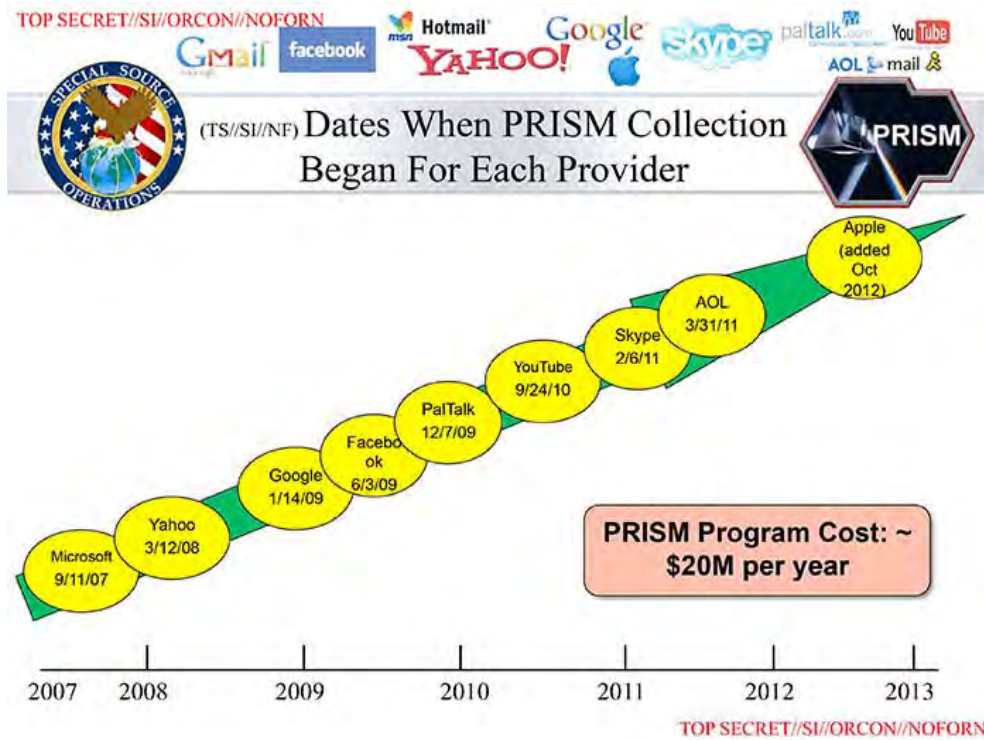
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Participating providers

This slide shows when each company joined the program, with Microsoft being the first, on Sept. 11, 2007, and Apple the most recent, in October 2012.



716 COMMENTS

Comment

Type your comment here

Sort:



thymorgans

1:21 PM PDT

Beginning in about 2008 someone.....someone carrying a Beijing internet protocol address tried to get into this old computer and was blocked by AOL and its firewall.....tried it for weeks.

Reply



thymorgans

1:21 PM PDT

Beginning in about 2008 someone.....someone carrying a Beijing internet protocol address tried to get into this old computer and was blocked by AOL and its firewall.....tried it for weeks.

Reply



thymorgans

1:11 PM PDT

Mr. Edward Snowden will probably be found in Beijing.....Chinas prime data mining internet protocol address.

Reply



thymorgans

1:06 PM PDT

No surprise. Wrote my first computer program for the IBM type 650 in 1957.

RELATED STORIES

Whistleblower protections and the NSA leaks

Josh Hicks

The Federal Eye examines whistleblower protections for the intelligence community and how they relate to the recent disclosures.

Public reaction to NSA monitoring

The public backs giving the federal government broad authority to investigate terrorist threats, even extending to the phone record monitoring program of the NSA. Nearly half of all Americans say it's OK to monitor everyone's email if officials say this might avert an attack.

Sales of '1984' spike after NSA revelations

NSA head: 'Dozens' of terror events prevented

NSA director says surveillance programs thwarted 'dozens' of attacks

NSA chief: Forces must protect 'privacy' and national security

Senators ask NSA to declassify some information

ACLU sues over NSA surveillance program

EXHIBIT P

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF)

FAA702 Operations

Two Types of Collection



Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.
- (FAIRVIEW, ██████████, BLARNEY, ██████████)

You Should Use Both

PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

TOP SECRET//SI//ORCON//NOFORN