14-42

IN THE

United States Court of Appeals

FOR THE

Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs–Appellants,

– v. –

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

Defendants–Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JOINT APPENDIX

Volume 1 of 2 (JA001–JA257)

Christopher T. Dunn
Arthur N. Eisenburg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

Jameel Jaffer
Alex Abdo
Patrick Toomey
Brett Max Kaufman
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

JOINT APPENDIX

VOLUME ONE

CLOSED, APPEAL, ECF, RELATED

U.S. District Court
Southern District of New York (Foley Square)
CIVIL DOCKET FOR CASE #: 1:13-cv-03994-WHP

American Civil Liberties Union et al v. Clapper et al
Assigned to: Judge William H. Pauley, III
Related Case: 1:11-cv-07562-WHP
Cause: 28:1331 Fed. Question

Date Filed: 06/11/2013
Date Terminated: 12/27/2013
Jury Demand: None
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: U.S. Government Defendant

Plaintiff

American Civil Liberties Union

represented by **Laura Donohue**
Georgetown Law
5417 Duvall Drive
Bethesda, MD 20816
(202) 662-9455
Email: lkdonohue@law.georgetown.edu
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alexander Abraham Abdo
American Civil Liberties Union, Women's Rights Proj
125 Broad Street
New York, NY 10004
(212) 549-2500 x2517
Fax: (2120 549-2654
Email: aabdo@aclu.org
ATTORNEY TO BE NOTICED

Brett Max Kaufman
American Civil Liberties Union
125 Broad Street
New York, NY 10004
(212)-549-2603
Fax: (212)-549-2654
Email: bkaufman@aclu.org
ATTORNEY TO BE NOTICED

Catherine Newby Crump
American Civil Liberties Union Foundation (NYC)
125 Broad Street
18th Floor
New York, NY 10004
(212) 519-7806
Fax: (212) 549-2651
Email: ccrump@aclu.org
ATTORNEY TO BE NOTICED

Jameel Jaffer

American Civil Liberties Union Foundation
(NYC)
125 Broad Street
18th Floor
New York, NY 10004
(212) 549-7814
Fax: (212) 549-2629
Email: jjaffer@aclu.org
ATTORNEY TO BE NOTICED

Patrick Christopher Toomey
American Civil Liberties Union Foundation
(NYC)
125 Broad Street
18th Floor
New York, NY 10004
(212) 519-7816
Fax: (212) 549-2654
Email: ptoomey@aclu.org
ATTORNEY TO BE NOTICED

Plaintiff

American Civil Liberties Union Foundation represented by **Laura Donohue**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alexander Abraham Abdo
(See above for address)
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

New York Civil Liberties Union represented by **Laura Donohue**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

New York Civil Liberties Union Foundation represented by **Laura Donohue**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Arthur Nelson Eisenberg
New York Civil Liberties Union
125 Broad Street, 17th floor

New York, NY 10004
(212) 607-3300
Fax: (212) 607-3318
Email: arteisenberg@nyclu.org
ATTORNEY TO BE NOTICED

Christopher T Dunn
New York Civil Liberties Union
125 Broad Street, 17th floor
New York, NY 10004
(212) 344-3005
Fax: (212) 344-3318
Email: cdunn@nyclu.org
ATTORNEY TO BE NOTICED

Jameel Jaffer
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

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

represented by

Christopher Blake Harwood
United States Attorney's Office
Southern District Of New York
86 Chambers Street, Third Floor
New York, NY 10007
(212) 637-2728
Fax: (212) 637-2786
Email: christopher.harwood@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Dalton Clopper
U.S. Attorney's Office, SDNY
86 Chambers Street
New York, NY 10007
212 637 2716
Fax: 212 637 0033
Email: john.clopper@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tara Marie La Morte
U.S. Attorney's Office, SDNY (Chambers Street)
86 Chambers Street
New York, NY 10007
(212) 637-2746
Fax: (212) 637-2730
Email: tara.lamorte2@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

David Stuart Jones
U.S. Attorney's Office, SDNY (86 Chambers St.)
86 Chambers Street
New York, NY 10007
212-637-2200
Fax: 212-637-2686
Email: david.jones6@usdoj.gov
ATTORNEY TO BE NOTICED

Defendant

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

represented by **Christopher Blake Harwood**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Dalton Clopper
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tara Marie La Morte
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

David Stuart Jones
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

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

represented by **Christopher Blake Harwood**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Dalton Clopper
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tara Marie La Morte
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

David Stuart Jones
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

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

represented by **Christopher Blake Harwood**
(See above for address)
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

John Dalton Clopper
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tara Marie La Morte
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

David Stuart Jones
(See above for address)
ATTORNEY TO BE NOTICED

Defendant

Robert S. Mueller, III
in his official capacity as Director of the Federal Bureau of Investigation

represented by **Christopher Blake Harwood**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Dalton Clopper
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Tara Marie La Morte
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

David Stuart Jones
(See above for address)
ATTORNEY TO BE NOTICED

ADR Provider

Amicus Curiae Pen American Center

represented by **Edward J. Davis**
Davis Wright Tremaine LLP (NYC)
1633 Broadway
New York, NY 10019
(212) 489-8230
Fax: (212) 489-8340
Email: eddavis@dwt.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Amicus

Former Church Committee Members and Law Professors

represented by **Laura Donohue**
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Electronic Frontier Foundation

represented by

David Allen Greene
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415)-436-9333
Fax: (415)-436-9993
Email: davidg@eff.org
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

National Rifle Association of America, Inc.

represented by

John Frazer
Law Office of John Frazer, PLLC
3925 Chain Bridge Road, Suite 403
Fairfax, VA 22030
(703) 352-7276
Fax: (703) 359-0938
Email: jfrazer@jfrazerlaw.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

Professor Michael P. Lynch

represented by

David Benjamin Owens
Loevy & Loevy
312 N. May St., Suite 100
Hauppauge, NY 60607
(312)-243-5900
Fax: (312)-243-5902
Email: david@loevy.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

Reporters Committee for Freedom of the Press

represented by

Michael Douglas Steger
Steger Krane LLP
1601 Broadway, 12th Floor
New York, NY 10019
(212) 736-6800
Fax: (845) 689-2155
Email: msteger@steger-law.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Amicus

F. James Sensenbrenner

represented by

David Allen Greene
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Amicus

Pen American Center

represented by **Edward J. Davis**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Linda Jane Steinman
Davis Wright Tremaine LLP (NYC)
1633 Broadway
New York, NY 10019
212-603-6409
Fax: 212-489-8340
Email: lindasteinman@dwt.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Eric Joel Feder
Davis Wright Tremaine LLP (NYC)
1633 Broadway
New York, NY 10019
(212) 489-8230
Fax: (212) 489-8340
Email: ericfeder@dwt.com
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
06/11/2013	1	COMPLAINT against Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Filing Fee $ 350.00, Receipt Number 1069477)Document filed by American Civil Liberties Union Foundation, New York Civil Liberties Union Foundation, New York Civil Liberties Union, American Civil Liberties Union.(laq) (jd). (Entered: 06/12/2013)
06/11/2013		SUMMONS ISSUED as to Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (laq) (Entered: 06/12/2013)
06/11/2013		CASE REFERRED TO Judge William H. Pauley as possibly related to 1:11-cv-7562. (laq) (Entered: 06/12/2013)
06/11/2013		Case Designated ECF. (laq) (Entered: 06/12/2013)
06/14/2013		CASE ACCEPTED AS RELATED. Create association to 1:11-cv-07562-WHP. Notice of Assignment to follow. (pgu) (Entered: 06/14/2013)
06/14/2013	2	NOTICE OF CASE ASSIGNMENT to Judge William H. Pauley, III. Judge Unassigned is no longer assigned to the case. (pgu) (Entered: 06/14/2013)
06/14/2013		Magistrate Judge James L. Cott is so designated. (pgu) (Entered: 06/14/2013)
06/25/2013	3	AFFIDAVIT OF SERVICE. James R. Clapper served on 6/24/2013, answer due 7/15/2013. Service was made by Mail. Document filed by American Civil Liberties Union Foundation; New York Civil Liberties Union Foundation; New York Civil Liberties Union; American Civil Liberties Union. (Jaffer, Jameel) (Entered: 06/25/2013)
06/25/2013	4	AFFIDAVIT OF SERVICE. Charles T. Hagel served on 6/24/2013, answer due 7/15/2013. Service was made by Mail. Document filed by American Civil Liberties Union Foundation; New York Civil Liberties Union Foundation; New York Civil Liberties Union; American Civil Liberties Union. (Jaffer, Jameel) (Entered: 06/25/2013)
06/25/2013	5	

		AFFIDAVIT OF SERVICE. Eric H. Holder served on 6/24/2013, answer due 7/15/2013. Service was made by Mail. Document filed by American Civil Liberties Union Foundation; New York Civil Liberties Union Foundation; New York Civil Liberties Union; American Civil Liberties Union. (Jaffer, Jameel) (Entered: 06/25/2013)
06/25/2013	6	AFFIDAVIT OF SERVICE. Keith B. Alexander served on 6/24/2013, answer due 7/15/2013. Service was made by Mail. Document filed by American Civil Liberties Union Foundation; New York Civil Liberties Union Foundation; New York Civil Liberties Union; American Civil Liberties Union. (Jaffer, Jameel) (Entered: 06/25/2013)
06/25/2013	7	AFFIDAVIT OF SERVICE. Robert S. Mueller, III served on 6/24/2013, answer due 7/15/2013. Service was made by Mail. Document filed by American Civil Liberties Union Foundation; New York Civil Liberties Union Foundation; New York Civil Liberties Union; American Civil Liberties Union. (Jaffer, Jameel) (Entered: 06/25/2013)
06/25/2013	8	AFFIDAVIT OF SERVICE of Complaint and Summons served on U.S. Attorney for the Southern District of New York on 06/24/2013. Service was made by Mail. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Jaffer, Jameel) (Entered: 06/25/2013)
06/26/2013	9	NOTICE OF APPEARANCE by Tara Marie La Morte on behalf of Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (La Morte, Tara) (Entered: 06/26/2013)
06/27/2013	10	ORDER FOR INITIAL PRETRIAL CONFERENCE: Initial Conference set for 7/17/2013 at 02:00 PM in Courtroom 20B, 500 Pearl Street, New York, NY 10007 before Judge William H. Pauley III, and as further set forth in this document. (Signed by Judge William H. Pauley, III on 6/25/2013) Copies Sent By Chambers. (cd) (Entered: 06/27/2013)
07/03/2013	11	SCHEDULING ORDER: This initial pretrial conference scheduled for July 17, 2013 is rescheduled to July 25, 2013 at 12:00 p.m. (Signed by Judge William H. Pauley, III on 7/3/2013) Copies Sent by Chambers. (mro) (Entered: 07/03/2013)
07/03/2013	12	ENDORSED LETTER addressed to Judge William H. Pauley, III from Jameel Jaffer dated 7/2/13 re: Counsel writes to request a pre-motion conference to discuss a motion for a preliminary injunction. ENDORSEMENT: Application granted. The Court will hold a pre-motion conference in conjunction with the initial pre-trial conference, which has been rescheduled to July 25, 2013 at 12:00 p.m. (Pre-Motion Conference set for 7/25/2013 at 12:00 PM before Judge William H. Pauley III.) (Signed by Judge William H. Pauley, III on 7/3/2013) (mro) (Entered: 07/03/2013)
07/12/2013	13	ENDORSED LETTER addressed to Judge William H. Pauley, III from David S. Jones dated 7/9/13 re: Counsel writes respectfully with the consent of plaintiffs' counsel to request a one-week extension of defendants' time to respond to plaintiffs' July 2 pre-motion conference letter. ENDORSEMENT: Application granted. (Signed by Judge William H. Pauley, III on 7/11/2013) (mro) (Entered: 07/12/2013)
07/16/2013	14	NOTICE OF APPEARANCE by John Dalton Clopper on behalf of Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Clopper, John) (Entered: 07/16/2013)
07/16/2013	15	NOTICE OF APPEARANCE by David Stuart Jones on behalf of Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Jones, David) (Entered: 07/16/2013)
07/23/2013	16	ENDORSED LETTER addressed to Judge William H. Pauley, III from David S. Jones dated 7/18/13 re: Counsel writes in response to plaintiffs' July 2 letter requesting that the initial conference now scheduled for July 25 serve as a pre-motion conference in anticipation of a

		preliminary injunction motion. Defendants request that the same conference also serve as a pre-motion conference for a potential cross-motion to dismiss the complaint. For the reasons herein, counsel requests that defendants' initial briefing on these matters be due no earlier than September 16. ENDORSEMENT: Application granted in part. The July 25 conference will serve as a pre-motion conference for Defendants' anticipated motion to dismiss. The briefing schedule will be discussed at the conference. (Signed by Judge William H. Pauley, III on 7/22/2013) (mro) (Entered: 07/23/2013)
07/24/2013	17	**FILING ERROR - DEFICIENT DOCKET ENTRY -** NOTICE OF APPEARANCE by Christopher Blake Harwood on behalf of Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Harwood, Christopher) Modified on 7/24/2013 (db). (Entered: 07/24/2013)
07/24/2013		*****NOTE TO ATTORNEY TO RE-FILE DOCUMENT - DEFICIENT DOCKET ENTRY ERROR. Note to Attorney Christopher Blake Harwood to RE-FILE Document 17 Notice of Appearance. ERROR(S): Document has not been fully secured, items can be changed/altered in real time. (db)** (Entered: 07/24/2013)
07/24/2013	18	NOTICE OF APPEARANCE by Christopher Blake Harwood on behalf of Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Harwood, Christopher) (Entered: 07/24/2013)
07/25/2013	19	**FILING ERROR - DEFICIENT DOCKET ENTRY -** MOTION for Laura K. Donohue to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8723410. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Attachments: # 1 Civil Cover Sheet Cover, # 2 Text of Proposed Order Order, # 3 Supplement Certificate of Good Standing)(Donohue, Laura) Modified on 7/25/2013 (bcu). (Entered: 07/25/2013)
07/25/2013		**>>>NOTICE REGARDING DEFICIENT MOTION TO APPEAR PRO HAC VICE. Notice regarding Document No. 19 MOTION for Laura K. Donohue to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8723410. Motion and supporting papers to be reviewed by Clerk's Office staff.. The filing is deficient for the following reason(s): Missing Certificate of Good Standing. Certificate of Good Standing must be issued from the State Court of Virginia not from a State Bar Association. Re-file the document as a Corrected Motion to Appear Pro Hac Vice and attach a valid Certificate of Good Standing, issued within the past 30 days. (bcu)** (Entered: 07/25/2013)
07/26/2013	20	SCHEDULING ORDER: Counsel for the parties having appeared for a conference on July 25, 2013, the following schedule is established: 1. Plaintiffs will file a motion for a preliminary injunction and Defendants will file a motion to dismiss by August 26, 2013; 2. Opposition briefs are due September 26, 2013; 3. Third parties may file motions for leave to file amici briefs by October 3, 2013 with their proposed briefs attached; 4. Reply briefs are due October 10, 2013; 5. The Court will hear oral argument on November 1, 2013 at 12:00 p.m; 6. Moving and opposition briefs may be 40 pages in length, reply briefs may be 20 pages. (Signed by Judge William H. Pauley, III on 7/25/2013) Copies Sent by Chambers. (mro) (Entered: 07/26/2013)
07/26/2013		Set/Reset Hearings: Oral Argument set for 11/1/2013 at 12:00 PM before Judge William H. Pauley III. (mro) (Entered: 07/26/2013)
07/26/2013	21	LETTER addressed to Judge William H. Pauley from David S. Jones dated 7/18/2013 re: Pursuant to the court's order dated June 27, 2013, I write respectfully on behalf of both parties concerning matters covered by Rule 26(f) of the parties' discovery plan. (ama) (Entered: 07/29/2013)
08/08/2013	22	CORRECTED SCHEDULING ORDER: By letter dated August 2, 2013, the ACLU brought to the Court's attention an error in this Court's July 26, 2013 Scheduling Order. The Court therefore adopts the following corrected schedule: 1. Plaintiffs will file a motion for a

		preliminary injunction and Defendants will file a motion to dismiss by August 26, 2013; 2. Third parties may file motions for leave to file amici briefs by September 4, 2013 with their proposed briefs attached; 3. Opposition briefs are due September 26, 2013; 4. Reply briefs are due October 10, 2013; 5. The Court will hear oral argument on November 1, 2013 at 12:00 p.m; 6. Moving and opposition briefs may be 40 pages in length, reply briefs may be 20 pages. (Motions due by 9/4/2013. Responses due by 9/26/2013 Replies due by 10/10/2013. Oral Argument set for 11/1/2013 at 12:00 PM before Judge William H. Pauley III.) (Signed by Judge William H. Pauley, III on 8/8/2013) Copies Sent By Chambers. (mro) (Entered: 08/08/2013)
08/23/2013	23	SECOND MOTION for Laura Kathleen Donohue to Appear Pro Hac Vice. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by Former Church Committee Members and Law Professors. (Attachments: # 1 Text of Proposed Order, # 2 Exhibit Certificate of Good Standing with the Virginia Bar, # 3 Certificate of Good Standing Virginia Supreme Court)(Donohue, Laura) (Entered: 08/23/2013)
08/23/2013		**>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 23 SECOND MOTION for Laura Kathleen Donohue to Appear Pro Hac Vice. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (wb)** (Entered: 08/23/2013)
08/26/2013	24	MOTION for David Allen Greene to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8816230. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by Electronic Frontier Foundation. (Attachments: # 1 Text of Proposed Order, # 2 Certificate of Good Standing)(Greene, David) (Entered: 08/26/2013)
08/26/2013		**>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 24 MOTION for David Allen Greene to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8816230. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu)** (Entered: 08/26/2013)
08/26/2013	25	MOTION for Preliminary Injunction. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. Return Date set for 11/1/2013 at 12:00 PM.(Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	26	MEMORANDUM OF LAW in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	27	DECLARATION of Prof. Edward Felten in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	28	DECLARATION of Michael German in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	29	DECLARATION of Steven Shapiro in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	30	DECLARATION of Christopher Dunn in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union

		Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	31	DECLARATION of Patrick Toomey in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Abdo, Alexander) (Entered: 08/26/2013)
08/26/2013	32	MOTION to Dismiss. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. Responses due by 9/26/2013(Jones, David) (Entered: 08/26/2013)
08/26/2013	33	MEMORANDUM OF LAW in Support re: 32 MOTION to Dismiss.. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6, # 7 Exhibit 7, # 8 Exhibit 8, # 9 Exhibit 9, # 10 Exhibit 10, # 11 Exhibit 11, # 12 Exhibit 12, # 13 Exhibit 13)(Jones, David) (Entered: 08/26/2013)
08/27/2013	34	MOTION for John Frazer to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8817400. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by National Rifle Association of America, Inc.. (Attachments: # 1 Text of Proposed Order Proposed order for admission, # 2 Exhibit Certificate of good standing)(Frazer, John) (Entered: 08/27/2013)
08/27/2013	35	ORDER FOR ADMISSION PRO HAC VICE granting 23 Motion for Laura K. Donohue to Appear Pro Hac Vice. (Signed by Judge William H. Pauley, III on 8/27/2013) (tro) (Entered: 08/27/2013)
08/27/2013		**>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 34 MOTION for John Frazer to Appear Pro Hac Vice. Filing fee $ 200.00, receipt number 0208-8817400. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu)** (Entered: 08/27/2013)
08/28/2013	36	ORDER FOR ADMISSION PRO HAC VICE granting 24 Motion for David A. Greene to Appear Pro Hac Vice. It is hereby Ordered that David A. Greene is admitted pro hac vice to appear for all purposes as counsel for amicus curiae Electronic Frontier Foundation. (Signed by Judge William H. Pauley, III on 8/28/2013) (mro) (Entered: 08/28/2013)
08/28/2013	37	ORDER FOR ADMISSION PRO HAC VICE granting 34 Motion for John Frazer to Appear Pro Hac Vice. IT IS HEREBY ORDERED that John Frazer is admitted pro hac vice to appear for all purposes as counsel for amicus curiae National Rifle Association of America, Inc. (Signed by Judge William H. Pauley, III on 8/26/2013) (mro) (Entered: 08/28/2013)
08/29/2013	38	**FILING ERROR - DEFICIENT DOCKET ENTRY -** MOTION for David B. Owens to Appear Pro Hac Vice *for amicus curiae Michael P. Lynch*. Filing fee $ 200.00, receipt number 0208-8827772. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by Michael P. Lynch. (Attachments: # 1 Text of Proposed Order Proposed Order For Pro Hac Vice Admission, # 2 Exhibit Certificate of Good Standing (California), # 3 Exhibit Certificate of Good Standing (Illinois))(Owens, David) Modified on 8/29/2013 (bcu). (Entered: 08/29/2013)
08/29/2013		**>>>NOTICE REGARDING DEFICIENT MOTION TO APPEAR PRO HAC VICE. Notice regarding Document No. 38 MOTION for David B. Owens to Appear Pro Hac Vice *for amicus curiae Michael P. Lynch*. Filing fee $ 200.00, receipt number 0208-8827772. Motion and supporting papers to be reviewed by Clerk's Office staff.. The filing is deficient for the following reason(s): Missing Certificate of Good Standing. Certificate of Good Standing must be issued from the Supreme Court of California not from a State Bar Association. Re-file the document as a Corrected Motion to Appear Pro Hac Vice and**

		attach a valid Certificate of Good Standing, issued within the past 30 days. (bcu) (Entered: 08/29/2013)
08/30/2013	39	FIRST MOTION for Leave to File Motion for Leave to File Amicus Brief. Document filed by Former Church Committee Members and Law Professors. Return Date set for 8/30/2013 at 12:26 PM. (Attachments: # 1 Supplement Certificate of Service, # 2 Exhibit Amicus Brief) (Donohue, Laura) (Entered: 08/30/2013)
09/03/2013	40	AMENDED MOTION for David B. Owens to Appear Pro Hac Vice *on behalf of Michael P. Lynch (amicus curiae)*. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by Michael P. Lynch. (Attachments: # 1 Exhibit Certificate of Good Standing (California), # 2 Exhibit Certificate of Good Standing (Illinois), # 3 Text of Proposed Order)(Owens, David) (Entered: 09/03/2013)
09/03/2013		**>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 40 AMENDED MOTION for David B. Owens to Appear Pro Hac Vice *on behalf of Michael P. Lynch (amicus curiae)*. Motion and supporting papers to be reviewed by Clerk's Office staff.AMENDED MOTION for David B. Owens to Appear Pro Hac Vice *on behalf of Michael P. Lynch (amicus curiae)*. Motion and supporting papers to be reviewed by Clerk's Office staff.. The document has been reviewed and there are no deficiencies. (bcu)** (Entered: 09/03/2013)
09/04/2013	41	ORDER FOR ADMISSION PRO HAC VICE granting 40 Motion for David B. Owens to Appear Pro Hac Vice. (Signed by Judge William H. Pauley, III on 9/4/2013) (lmb) (Entered: 09/04/2013)
09/04/2013	42	MOTION for Leave to File *Amicus Brief*. Document filed by Reporters Committee for Freedom of the Press. (Attachments: # 1 Proposed brief, # 2 Appendix Apprendix A, # 3 Appendix Appendix B)(Steger, Michael) (Entered: 09/04/2013)
09/04/2013	43	MOTION for David Allen Greene to Appear Pro Hac Vice *(Corrected)*. **Motion and supporting papers to be reviewed by Clerk's Office staff.** Document filed by F. James Sensenbrenner. (Attachments: # 1 Text of Proposed Order, # 2 Certificate of Good Standing) (Greene, David) (Entered: 09/04/2013)
09/04/2013	44	MOTION for Leave to File Amicus brief. Document filed by National Rifle Association of America, Inc.. (Attachments: # 1 Exhibit Amicus brief)(Frazer, John) (Entered: 09/04/2013)
09/04/2013	45	MOTION for Leave to File Amicus Brief *by Professor of Philosophy, Michael P. Lynch*. Document filed by Michael P. Lynch. (Attachments: # 1 Proposed Brief)(Owens, David) (Entered: 09/04/2013)
09/04/2013	46	MOTION for Leave to File Amicus Curiae Brief *in Support of Plaintiffs*. Document filed by F. James Sensenbrenner. (Attachments: # 1 Exhibit A (Amicus Brief), # 2 Text of Proposed Order) (Greene, David) (Entered: 09/04/2013)
09/04/2013	47	MOTION for Leave to File Motion of Non-Party PEN American Center for Leave to File Brief as Amicus Curiae in support of Plaintiffs. Document filed by Pen American Center. (Attachments: # 1 Exhibit Proposed Amicus Brief, # 2 Exhibit Certificate of Service)(Davis, Edward) (Entered: 09/04/2013)
09/04/2013	48	NOTICE OF APPEARANCE by Edward J. Davis on behalf of Pen American Center. (Davis, Edward) (Entered: 09/04/2013)
09/04/2013	49	NOTICE OF APPEARANCE by Linda Jane Steinman on behalf of Pen American Center. (Steinman, Linda) (Entered: 09/04/2013)
09/04/2013	50	NOTICE OF APPEARANCE by Eric Joel Feder on behalf of Pen American Center. (Feder, Eric) (Entered: 09/04/2013)
09/05/2013		

		>>>NOTICE REGARDING PRO HAC VICE MOTION. Regarding Document No. 43 MOTION for David Allen Greene to Appear Pro Hac Vice *(Corrected)*. Motion and supporting papers to be reviewed by Clerk's Office staff. MOTION for David Allen Greene to Appear Pro Hac Vice *(Corrected)*. Motion and supporting papers to be reviewed by Clerk's Office staff. The document has been reviewed and there are no deficiencies. (bwa) (Entered: 09/05/2013)
09/05/2013	51	ORDER granting 39 Motion for Leave to File Document; granting 42 Motion for Leave to File Document; granting 44 Motion for Leave to File Document; granting 45 Motion for Leave to File Document; granting 46 Motion for Leave to File Document; granting 47 Motion for Leave to File Document. The motions of amicus curiae Former Members of the Church Committee and Law Professors; The Reporters Committee for Freedom of the Press, et. al.; the National Rifle Association of America, Inc.; Michael P. Lynch; Representative F. James Sensenbrenner, Jr.; and the PEN American Center are granted. Amicus curiae may file their proposed briefs. The Clerk of Court is directed to terminate the motions pending at Docket Nos. 39, 42, 44, 45, 46, and 47. (Signed by Judge William H. Pauley, III on 9/5/2013) (mro) (Entered: 09/05/2013)
09/05/2013	52	ORDER FOR ADMISSION PRO HAC VICE granting 43 Motion for David A. Greene to Appear Pro Hac Vice. It is hereby Ordered that David A. Greene is admitted pro hac vice to appear for all purposes as counsel for amicus curiae Congressman Jim Sensenbrenner. (Signed by Judge William H. Pauley, III on 9/5/2013) (mro) (Entered: 09/05/2013)
09/05/2013	53	BRIEF *OF AMICUS CURIAE PEN AMERICAN CENTER IN SUPPORT OF PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION AND IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS*. Document filed by Pen American Center.(Davis, Edward) (Entered: 09/05/2013)
09/05/2013	54	BRIEF *OF AMICUS CURIAE*. Document filed by National Rifle Association of America, Inc.. (Frazer, John) (Entered: 09/05/2013)
09/05/2013	55	BRIEF *of Amicus Curiae Professor Michael P. Lynch*. Document filed by Michael P. Lynch. (Owens, David) (Entered: 09/05/2013)
09/06/2013	56	BRIEF *Amicus Curiae in Suppport of Plaintiffs*. Document filed by F. James Sensenbrenner. (Greene, David) (Entered: 09/06/2013)
09/26/2013	57	LETTER MOTION for Extension of Time to File Response/Reply as to 32 MOTION to Dismiss., 25 MOTION for Preliminary Injunction. addressed to Judge William H. Pauley, III from David S. Jones dated September 26, 2013. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Attachments: # 1 Text of Proposed Order Proposed revised scheduling order)(Jones, David) (Entered: 09/26/2013)
09/27/2013	58	REVISED SCHEDULING ORDER: It is hereby ORDERED that (a) plaintiffs' opposition to defendants' motion to dismiss and defendants' opposition to plaintiffs' motion for a preliminary injunction shall be due on or before October 1, 2013, and (b) plaintiffs' and defendants' reply papers in further support of their respective motions shall be due on or before October 15, 2013. Set Deadlines/Hearing as to 25 MOTION for Preliminary Injunction., 32 MOTION to Dismiss : (Responses due by 10/1/2013, Replies due by 10/15/2013.) (Signed by Judge William H. Pauley, III on 9/27/2013) (mro) (Entered: 09/27/2013)
10/01/2013	59	STANDING ORDER M10-468: Stay of Certain Civil Cases Pending the Restoration of Department of Justice Funding. (Signed by Judge Loretta A. Preska on 10/1/2013) ***Original Standing Order docketed in case no. 1:13-mc-00334-LAP, document no. 2 on 10/1/2013.*** (tro) (Entered: 10/01/2013)
10/01/2013	60	MEMORANDUM OF LAW in Opposition re: 32 MOTION to Dismiss.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Jaffer, Jameel) (Entered: 10/01/2013)

10/01/2013	61	MEMORANDUM OF LAW in Opposition re: 25 MOTION for Preliminary Injunction.. Document filed by Keith B. Alexander. (Attachments: # 1 Exhibit)(Jones, David) (Entered: 10/01/2013)
10/01/2013	62	DECLARATION of Robert J. Holley in Opposition re: 25 MOTION for Preliminary Injunction.. Document filed by Keith B. Alexander. (Jones, David) (Entered: 10/01/2013)
10/01/2013	63	DECLARATION of Teresa H. Shea in Opposition re: 25 MOTION for Preliminary Injunction.. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Jones, David) (Entered: 10/01/2013)
10/10/2013	64	LETTER MOTION for Extension of Time *& to Lift Stay* addressed to Judge William H. Pauley, III from Jameel Jaffer dated 10/10/13. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Attachments: # 1 Text of Proposed Order)(Jaffer, Jameel) (Entered: 10/10/2013)
10/11/2013	65	LETTER RESPONSE in Opposition to Motion addressed to Judge William H. Pauley, III from David S. Jones dated 10/11/2013 re: 64 LETTER MOTION for Extension of Time *& to Lift Stay* addressed to Judge William H. Pauley, III from Jameel Jaffer dated 10/10/13.. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Jones, David) (Entered: 10/11/2013)
10/11/2013	66	LETTER RESPONSE to Motion addressed to Judge William H. Pauley, III from David S. Jones dated 10/11/2013 re: 64 LETTER MOTION for Extension of Time *& to Lift Stay* addressed to Judge William H. Pauley, III from Jameel Jaffer dated 10/10/13. *Corrected version of dkt no 65, correcting nonsubstantive typographical error*. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Jones, David) (Entered: 10/11/2013)
10/15/2013	67	ORDER granting 64 Letter Motion for Extension of Time. Accordingly, the stay is lifted and the Court adopts the following schedule: 1. The parties will file reply briefs on their pending motions on October 25, 2013; 2. This Court will hear oral argument on November 22, 2013 at 10:30 a.m. (Signed by Judge William H. Pauley, III on 10/15/2013) (mro) (Entered: 10/15/2013)
10/15/2013		Set/Reset Deadlines: (Replies due by 10/25/2013.), Set/Reset Hearings:(Oral Argument set for 11/22/2013 at 10:30 AM before Judge William H. Pauley III.) (mro) (Entered: 10/15/2013)
10/25/2013	68	REPLY MEMORANDUM OF LAW in Support re: 25 MOTION for Preliminary Injunction.. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Attachments: # 1 Affidavit)(Jaffer, Jameel) (Entered: 10/25/2013)
10/25/2013	69	REPLY MEMORANDUM OF LAW in Support re: 32 MOTION to Dismiss.. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Attachments: # 1 Exhibit, # 2 Exhibit)(Jones, David) (Entered: 10/25/2013)
10/28/2013	70	LETTER addressed to Judge William H. Pauley, III from Jameel Jaffer dated 10/28/2013 re: Pls.' Reply, Pursuant to Rule III(F). Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation.(Jaffer, Jameel) (Entered: 10/28/2013)
10/29/2013	71	LETTER addressed to Judge William H. Pauley, III from David S. Jones dated 10/29/2013 re: listing documents filed in connection with defendants' motion to dismiss. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Jones, David) (Entered: 10/29/2013)
11/21/2013	72	RESPONSE in Support of Motion re: 32 MOTION to Dismiss., 25 MOTION for Preliminary Injunction. *Letter to Court (i) notifying parties of appearance by Assistant Attorney General*

		Stuart F. Delery, and (ii) identifying recently published decisions relevant to pending motions. Document filed by Keith B. Alexander, James R. Clapper, Charles T. Hagel, Eric H. Holder, Robert S. Mueller, III. (Attachments: # 1 Exhibit Ex. B - S.D. Cal. decision)(Jones, David) (Entered: 11/21/2013)
12/05/2013	73	TRANSCRIPT of Proceedings re: ARGUMENT held on 11/22/2013 before Judge William H. Pauley, III. Court Reporter/Transcriber: Eve Giniger, (212) 805-0300. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained through PACER. Redaction Request due 12/30/2013. Redacted Transcript Deadline set for 1/9/2014. Release of Transcript Restriction set for 3/10/2014.(Rodriguez, Somari) (Entered: 12/05/2013)
12/05/2013	74	NOTICE OF FILING OF OFFICIAL TRANSCRIPT Notice is hereby given that an official transcript of a ARGUMENT proceeding held on 11/22/13 has been filed by the court reporter/transcriber in the above-captioned matter. The parties have seven (7) calendar days to file with the court a Notice of Intent to Request Redaction of this transcript. If no such Notice is filed, the transcript may be made remotely electronically available to the public without redaction after 90 calendar days...(Rodriguez, Somari) (Entered: 12/05/2013)
12/16/2013	75	LETTER addressed to Judge William H. Pauley, III from Jameel Jaffer dated 12/16/2013 re: Notice of Supplemental Authority. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. (Attachments: # 1 Exhibit Klayman v. Obama (D.D.C. Dec. 16, 2013))(Jaffer, Jameel) (Entered: 12/16/2013)
12/27/2013	76	MEMORANDUM & ORDER denying 25 Motion for Preliminary Injunction; granting 32 Motion to Dismiss. For all of the reasons herein, the NSA's bulk telephony metadata collection program is lawful. Accordingly, the Government's motion to dismiss the complaint is granted and the ACLU's motion for a preliminary injunction is denied. The Clerk of Court is directed to terminate the motions pending at ECF Nos. 25 and 32 and to mark this case closed. (Signed by Judge William H. Pauley, III on 12/27/2013) (mro) (Main Document 76 replaced on 1/7/2014) (lmb). (Entered: 12/27/2013)
12/27/2013		Transmission to Judgments and Orders Clerk. Transmitted re: 76 Order on Motion for Preliminary Injunction, Order on Motion to Dismiss,,,,,, to the Judgments and Orders Clerk. (mro) (Entered: 12/27/2013)
12/27/2013	77	CLERK'S JUDGMENT That for the reasons stated in the Court's Memorandum and Order dated December 27, 2013, the Court finds the NSA's bulk telephony metadata collection program is lawful; accordingly, the Governments motion to dismiss the complaint is granted and the ACLU's motion for a preliminary injunction is denied and the case is closed. (Signed by Clerk of Court Ruby Krajick on 12/27/13) (Attachments: # 1 Notice of Right to Appeal)(ml) (Entered: 12/27/2013)
01/02/2014	78	NOTICE OF APPEAL from 76 Order on Motion for Preliminary Injunction, Order on Motion to Dismiss,,,, 77 Clerk's Judgment,. Document filed by American Civil Liberties Union, American Civil Liberties Union Foundation, New York Civil Liberties Union, New York Civil Liberties Union Foundation. Filing fee $ 505.00, receipt number 0208-9221894. Form C and Form D are due within 14 days to the Court of Appeals, Second Circuit. (Jaffer, Jameel) (Entered: 01/02/2014)
01/06/2014		Transmission of Notice of Appeal and Certified Copy of Docket Sheet to US Court of Appeals re: 78 Notice of Appeal. (tp) (Entered: 01/06/2014)
01/06/2014		Appeal Record Sent to USCA (Electronic File). Certified Indexed record on Appeal Electronic Files (ONLY) for 78 Notice of Appeal, filed by New York Civil Liberties Union Foundation, New York Civil Liberties Union, American Civil Liberties Union, American Civil Liberties Union Foundation were transmitted to the U.S. Court of Appeals. (tp) (Entered: 01/06/2014)

PACER Service Center			
Transaction Receipt			
03/03/2014 17:04:44			
PACER Login:	ac0937	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	1:13-cv-03994-WHP
Billable Pages:	15	**Cost:**	1.50

13 CV 3994

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

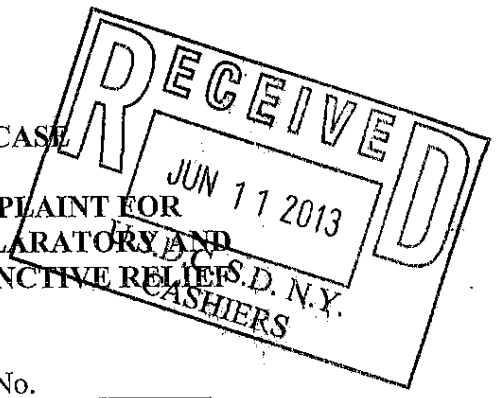
AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

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

Defendants.



ECF CASE

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Case No. _____

Hon. _____

Arthur N. Eisenberg (AE-2012)
Christopher T. Dunn (CD-3991)
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

Jameel Jaffer (JJ-4653)
Alex Abdo (AA-0527)
Brett Max Kaufman (BK-2827)
Patrick Toomey (PT-1452)
Catherine Crump (CC-4067)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

June 11, 2013

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

1. This lawsuit challenges the government's dragnet acquisition of Plaintiffs' telephone records under Section 215 of the Patriot Act, 50 U.S.C. § 1861.[1] In response to information published by the media, the government has acknowledged that it is relying on Section 215 to collect "metadata" about every phone call made or received by residents of the United States. The practice is akin to snatching every American's address book—with annotations detailing whom we spoke to, when we talked, for how long, and from where. It gives the government a comprehensive record of our associations and public movements, revealing a wealth of detail about our familial, political, professional, religious, and intimate associations.

2. The government has confirmed the authenticity of an order issued six weeks ago by the Foreign Intelligence Surveillance Court ("FISC") requiring Verizon Business Network Services Inc. ("VBNS") to turn over, every day, metadata about the calls made by each of its subscribers over the three-month period ending on July 19, 2013. Government officials have indicated that the VBNS order is part of a program that has been in place for seven years and that collects records of all telephone communications of every customer of a major phone company, including Verizon, AT&T, and Sprint.

3. Plaintiffs the American Civil Liberties Union and the American Civil Liberties Union Foundation are current VBNS subscribers whose communications have already been monitored by the government under the VBNS order and whose communications continue to be monitored under that order now. Plaintiffs the New York Civil Liberties Union and the New York Civil Liberties Union Foundation are former customers of VBNS whose contract of service recently expired but whose telephony metadata likely remains in government databases. The

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

government's surveillance of their communications (hereinafter "Mass Call Tracking") allows the government to learn sensitive and privileged information about their work and clients, and it is likely to have a chilling effect on whistleblowers and others who would otherwise contact Plaintiffs for legal assistance. This surveillance is not authorized by Section 215 and violates the First and Fourth Amendments. Plaintiffs bring this suit to obtain a declaration that the Mass Call Tracking is unlawful; to enjoin the government from continuing the Mass Call Tracking under the VBNS order or any successor thereto; and to require the government to purge from its databases all of the call records related to Plaintiffs' communications collected pursuant to the Mass Call Tracking.

JURISDICTION AND VENUE

4. This case arises under the Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331. The Court also has jurisdiction under the Administrative Procedure Act, 5 U.S.C. § 702. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412.

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

PLAINTIFFS

6. The American Civil Liberties Union ("ACLU") is a 501(c)(4) non-profit, non-partisan organization that engages in public education and lobbying about the constitutional principles of liberty and equality. The ACLU has more than 500,000 members, including members in every state. The ACLU is incorporated in Washington, D.C. and has its principal place of business in New York City.

7. The American Civil Liberties Union Foundation ("ACLUF") is a 501(c)(3) organization that educates the public about civil-liberties issues and employs lawyers who provide legal representation free of charge in cases involving civil liberties. It is incorporated in New York State and has its principal place of business in New York City.

8. The New York Civil Liberties Union ("NYCLU") is a 501(c)(4) non-profit, non-partisan organization that functions as the ACLU affiliate in New York and that has as its mission the advancement and protection of civil liberties and civil rights. The NYCLU is incorporated in New York and has its principal place of business in New York City.

9. The New York Civil Liberties Union Foundation ("NYCLUF") is a 501(c)(3) non-profit, non-partisan organization whose mission is to defend civil rights and civil liberties and to preserve and extend constitutionally guaranteed rights to people whose rights have historically been denied. The NYCLUF provides counsel in lawsuits seeking to advance civil liberties and civil rights. It is incorporated in Delaware and has its principal place of business in New York City.

DEFENDANTS

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

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

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

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

14. Defendant Robert S. Mueller III is the Director of the FBI and is responsible for applications made to the FISC under Section 215 of the Patriot Act.

BACKGROUND

The Foreign Intelligence Surveillance Act

15. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern surveillance conducted for foreign-intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC"), a court composed of seven (now eleven) federal district court judges, and empowered the court to grant or deny government applications for surveillance orders in foreign-intelligence investigations.

16. Congress enacted FISA after years of in-depth congressional investigation by the committees chaired by Senator Frank Church and Representative Otis Pike, which revealed that the Executive Branch had engaged in widespread warrantless surveillance of United States citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."

Section 215 of the Patriot Act

17. Section 215 of the Patriot Act is often referred to as FISA's "business records" provision. When originally enacted in 1998, this provision permitted the FBI to apply to the FISC for an order to obtain business records of hotels, motels, car and truck rental agencies, and storage rental facilities.

18. Section 215 broadened this authority by eliminating any limitation on the types of businesses or entities whose records may be seized. In addition, Section 215 expanded the scope of the items that the FBI may obtain using this authority from "records" to "any tangible things (including books, records, papers, documents, and other items)."

19. Section 215 also relaxed the standard that the FBI is required to meet to obtain an order to seize these records. Previously, FISA required the FBI to present to the FISC "specific and articulable facts giving reason to believe that the person to whom the records pertain [was] a foreign power or an agent of a foreign power." In its current form, Section 215 requires only that the records or things sought be "relevant" to an authorized investigation "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."

20. Production orders issued under Section 215 are accompanied by gag orders generally forbidding recipients from revealing "that the Federal Bureau of Investigation has sought or obtained tangible things." Recipients may challenge gag orders "[n]ot less than 1 year after the date of the issuance of the production order." If a recipient challenges a gag order, the FISC must treat the government's claim "that disclosure may endanger the national security of the United States or interfere with diplomatic relations . . . as conclusive."

21. For the past several years, members of Congress have been warning the public that the Executive Branch was exceeding the limits of the Patriot Act. In 2009, Senator Russ Feingold stated during a hearing that "there . . . is information about the use of Section 215 orders that I believe Congress and the American people deserve to know," adding later that "Section 215 has been misused." In 2011, Senator Ron Wyden declared, "When the American people find out how their government has secretly interpreted the Patriot Act, they will be

stunned and they will be angry." Similarly, Senator Mark Udall protested that "Americans would be alarmed if they knew how this law is being carried out."

22. On June 5, 2013, *The Guardian* disclosed that, under Section 215, the NSA has been acquiring the metadata for every phone call made or received by customers of VBNS "on an ongoing daily basis."

23. Since the disclosure of the VBNS order last week and the government's official acknowledgement of it, the outcry in Congress has increased sharply. Representative Jim Sensenbrenner, an author of the Patriot Act and chairman of the House Judiciary Committee at the time of Section 215's passage, called the Section 215 surveillance program "an abuse of that law." He wrote that, "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."

PLAINTIFFS' ALLEGATIONS

24. Plaintiffs are non-profit organizations that engage in public education, lobbying, and pro bono litigation upholding the civil rights and liberties guaranteed by the Constitution. Collectively, Plaintiffs have more than 500,000 members, including members in every state. Plaintiffs' employees routinely communicate by phone with each other as well as with journalists, current and potential clients, legislators and legislative staff, and members of the public. These communications relate to Plaintiffs' advocacy, representation of clients, and efforts to lobby Congress. Plaintiffs' communications are sensitive and often privileged.

25. For example, Plaintiffs frequently place or receive phone calls from individuals relating to potential legal representation in suits against the federal government or state governments. Often, the mere fact that Plaintiffs have communicated with these individuals is sensitive or privileged.

26. In ongoing litigation, Plaintiffs often communicate with potential witnesses, informants, or sources who regard the fact of their association or affiliation with Plaintiffs as confidential. Particularly in their work relating to national security, access to reproductive services, racial discrimination, the rights of immigrants, and discrimination based on sexual orientation and gender identity, Plaintiffs' work often depends on their ability to keep even the fact of their discussions with certain individuals confidential.

27. Similarly, Plaintiffs often communicate with government and industry whistleblowers, lobbyists, journalists, and possible advocacy partners who consider the confidentiality of their associations with Plaintiffs essential to their work.

28. Plaintiffs ACLU and ACLUF are current customers of Verizon Business Network Services Inc. ("VBNS") and Verizon Wireless. VBNS provides the ACLU's and ACLUF's wired communications, including their landlines and internet connection. Verizon Wireless provides their wireless communications, including their mobile phones.

29. Plaintiff NYCLU was a customer of VBNS until early April 2013. Until that time, VBNS provided the NYCLU's wired communications, including their landlines.

30. On June 5, 2013, *The Guardian* published a FISC order directing VBNS to produce to the National Security Agency "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" of its customers' calls, including those "wholly within the United States." Secondary Order at 2, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISC Apr. 25, 2013), *available at* http://bit.ly/11FY393. The VBNS order was issued on April 25, 2013 and expires on July 19, 2013. The order was issued ex parte, and there is no procedure for Plaintiffs to challenge it in the FISC.

31. In the few days since *The Guardian* disclosed the VBNS order, government officials have revealed more about the government's surveillance under Section 215. On June 6, Defendant Clapper officially acknowledged the authenticity of the VBNS order and disclosed details about the broader program supported by the FISC's orders issued under Section 215. Among other things, he stated that: "[t]he judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation"; "[t]he only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls"; and "[t]he [FISC] reviews the program approximately every 90 days."

32. The following day, President Barack Obama also commented publicly on the Section 215 order. Like Defendant Clapper, the President acknowledged that the intelligence community is tracking phone numbers and the durations of calls.

33. Members of the congressional intelligence committees have confirmed that the order issued to VBNS was but a single, three-month order in a much broader, seven-year program that the government has relied upon to collect the telephone records of all Americans. Senator Dianne Feinstein has stated that "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 [FISC] under the business records section of the Patriot Act." Senator Saxby Chambliss has likewise stated that "[t]his has been going on for seven years."

34. News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans' call details extends beyond customers of VBNS, encompassing all wireless and landline subscribers of the country's three largest phone companies. *See* Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement with Verizon, AT&T and Sprint, the country's

three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total."); Siobhan Gorman & Jennifer Valentino-DeVries, *Government Is Tracking Verizon Customers' Records*, Wall St. J., June 6, 2013, http://on.wsj.com/13mLm7c ("The National Security Agency is obtaining a complete set of phone records from all Verizon U.S. customers under a secret court order, according to a published account and former officials.").

35. As customers of VBNS, Plaintiffs ACLU and ACLUF are covered by the now-public order of the FISC requiring VBNS to turn over *all* of its customers' call records—including all of Plaintiffs' call records—on an ongoing basis. Upon information and belief, Plaintiff NYCLU was covered by a similar order prior to the expiration of their contract with VBNS. Also upon information and belief, Plaintiffs ACLU and ACLUF are covered by a similar order directed to Verizon Wireless. The information collected includes Plaintiffs' numbers, the numbers of their contacts, the time and duration of every single call they placed or received, and the location of Plaintiffs and their contacts when talking on mobile phones. This information could readily be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil-liberties violations, as well as those whom Plaintiffs contact in connection with their work. The fact that the government is collecting this information is likely to have a chilling effect on people who would otherwise contact Plaintiffs.

CAUSES OF ACTION

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

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

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

PRAYER FOR RELIEF

WHEREFORE the plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over Plaintiffs' Complaint;

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

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

4. Permanently enjoin Defendants from continuing the Mass Call Tracking under the VBNS order or any successor thereto;

5. Order Defendants to purge from their possession all of the call records of Plaintiffs' communications in their possession collected pursuant to the Mass Call Tracking;

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

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

Respectfully submitted,

Arthur N. Eisenberg (AE-2012)
Christopher T. Dunn (CD-3991)
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300

Jameel Jaffer (JJ-4653)
Alex Abdo (AA-0527)
Brett Max Kaufman (BK-2827)
Patrick Toomey (PT-1452)
Catherine Crump (CC-4067)
American Civil Liberties Union Foundation

Fax: (212) 607-3318
aeisenberg@nyclu.org

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

June 11, 2013

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*,	:	13 Civ. 3994 (WHP)
Plaintiffs,	:	SCHEDULING ORDER
-against-	:	
JAMES R. CLAPPER, *et al.*	:	
Defendants.	:	

WILLIAM H. PAULEY III, District Judge:

Counsel for the parties having appeared for a conference on July 25, 2013, the following schedule is established:

1. Plaintiffs will file a motion for a preliminary injunction and Defendants will file a motion to dismiss by August 26, 2013;

2. Opposition briefs are due September 26, 2013;

3. Third parties may file motions for leave to file amici briefs by October 3, 2013 with their proposed briefs attached;

4. Reply briefs are due October 10, 2013;

5. The Court will hear oral argument on November 1, 2013 at 12:00 p.m;

6. Moving and opposition briefs may be 40 pages in length, reply briefs may be 20 pages.

Dated: July 25, 2013
New York, New York

SO ORDERED:

WILLIAM H. PAULEY III
U.S.D.J.

Copies to:

Jameel Jaffer, Esq.
Alex A. Abdo, Esq.
Brett M. Kaufman, Esq.
Patrick C. Toomey, Esq.
Catherine N. Crump, Esq.
125 Broad Street
New York, NY 10004

Arthur N. Eisenberg, Esq.
Christopher T. Dunn, Esq.
125 Broad Street, 17th Floor
New York, NY 10004
Counsel for Plaintiffs

Tara M. La Morte, Esq.
Christopher B. Harwood, Esq.
John D. Clopper, Esq.
David S. Jones, Esq.
U.S. Attorney's Office
86 Chambers Street
New York, NY 10007
Counsel for Defendants

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*,	:	13 Civ. 3994 (WHP)
Plaintiffs,	:	CORRECTED SCHEDULING ORDER
-against-	:	
JAMES R. CLAPPER, *et al.*	:	
Defendants.	:	

WILLIAM H. PAULEY III, District Judge:

By letter dated August 2, 2013, the ACLU brought to the Court's attention an error in this Court's July 26, 2013 Scheduling Order. The Court therefore adopts the following corrected schedule:

1. Plaintiffs will file a motion for a preliminary injunction and Defendants will file a motion to dismiss by August 26, 2013;

2. Third parties may file motions for leave to file amici briefs by September 4, 2013 with their proposed briefs attached;

3. Opposition briefs are due September 26, 2013;

4. Reply briefs are due October 10, 2013;

5. The Court will hear oral argument on November 1, 2013 at 12:00 p.m;

6. Moving and opposition briefs may be 40 pages in length, reply briefs may be 20 pages.

Dated: August 8, 2013
New York, New York

SO ORDERED:

WILLIAM H. PAULEY III
U.S.D.J.

Copies to:

Jameel Jaffer, Esq.
Alex A. Abdo, Esq.
Brett M. Kaufman, Esq.
Patrick C. Toomey, Esq.
Catherine N. Crump, Esq.
125 Broad Street
New York, NY 10004

Arthur N. Eisenberg, Esq.
Christopher T. Dunn, Esq.
125 Broad Street, 17th Floor
New York, NY 10004
Counsel for Plaintiffs

Tara M. La Morte, Esq.
Christopher B. Harwood, Esq.
John D. Clopper, Esq.
David S. Jones, Esq.
U.S. Attorney's Office
86 Chambers Street
New York, NY 10007
Counsel for Defendants

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**NOTICE OF MOTION FOR A PRELIMINARY INJUNCTION** No. 13-cv-03994 (WHP) **ECF CASE**

PLAINTIFFS' NOTICE OF MOTION FOR A PRELIMINARY INJUNCTION

Upon pleadings and papers in this matter, Plaintiffs now move this Court before the Honorable William H. Pauley III, United States District Court Judge, at the Daniel Patrick Moynihan United States Courthouse, 500 Pearl Street, New York, New York, for a preliminary injunction against the Defendants, their agents, servants, employees, officials, or any other person acting in concert with them or on their behalf, pursuant to Rule 65 of the Federal Rules of Civil Procedure.

In particular, Plaintiffs move this Court for a preliminary injunction that, during the pendency of this suit, (i) bars Defendants from collecting Plaintiffs' call records under the mass call-tracking program, (ii) requires Defendants to quarantine all of Plaintiffs' call records already collected under the program, and (iii) prohibits Defendants from querying metadata obtained through the program using any phone number or other identifier associated with Plaintiffs.

As set forth in the accompanying memorandum of law and declarations in support of this motion, and in the Complaint, Plaintiffs meet all of the requirements for the issuance of a preliminary injunction. Specifically, Plaintiffs submit:

1. Declaration of Professor Edward W. Felten, and the exhibit attached thereto;
2. Declaration of Steven R. Shapiro;
3. Declaration of Christopher Dunn;
4. Declaration of Michael German;
5. Declaration of Patrick C. Toomey, and the exhibits attached thereto;
6. Plaintiffs' Memorandum of Law.

The Court has scheduled oral argument at 12:00 p.m. on November 1, 2013. Plaintiffs respectfully request that this Court issue the preliminary injunction sought by the Plaintiffs pending a final resolution of the merits of the case.

Respectfully submitted,

/s/ Jameel Jaffer

Christopher T. Dunn (CD-3991)
Arthur N. Eisenberg (AE-2012)
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
aeisenberg@nyclu.org

Jameel Jaffer (JJ-4653)
Alex Abdo (AA-0527)
Brett Max Kaufman (BK-2827)
Patrick Toomey (PT-1452)
Catherine Crump (CC-4067)
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
jjaffer@aclu.org

August 26, 2013

CERTIFICATE OF SERVICE

I, Jameel Jaffer, certify that on August 26, 2013, I served the foregoing Motion for a Preliminary Injunction and accompanying papers upon Defendants, by operation of the Court's electronic filing system:

/s/ Jameel Jaffer
Jameel Jaffer

August 26, 2013

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**DECLARATION OF PROFESSOR EDWARD W. FELTEN** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF PROFESSOR EDWARD W. FELTEN

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

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

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

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

Biography

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

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

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

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

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

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

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

---

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

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

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

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

The Mass Call Tracking Program

9. On June 5, 2013, *The Guardian* disclosed an order issued by the Foreign Intelligence Surveillance Court ("FISC") pursuant to Section 215 of the Patriot Act (the "Verizon Order").[5] This order compelled a Verizon subsidiary, Verizon Business Network Services ("Verizon"), to produce to the National Security Agency ("NSA") on "an ongoing daily basis . . . all *call detail records* or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[6] The Director of National Intelligence subsequently acknowledged the authenticity of the Verizon Order.[7]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Metadata Is Easy to Analyze

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

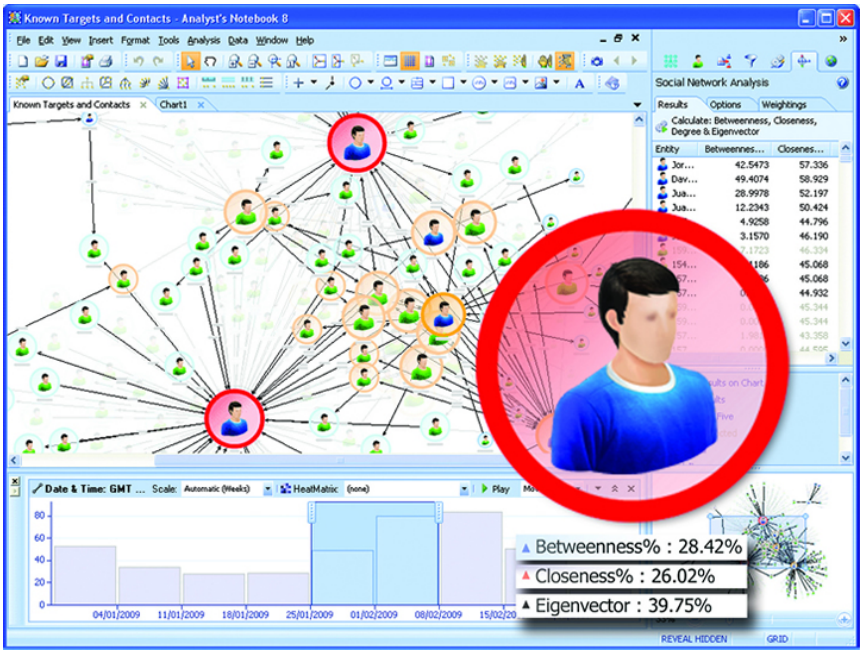


Figure 1: Screenshot of IBM's Analyst Notebook.[22]

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

[19] *Id.* at 4.

[20] *Id.* at 7.

[21] *Id.*

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

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

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

The Creation of Metadata Is Unavoidable

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

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

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

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

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

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

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

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

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

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

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

Telephony Metadata Reveals Content

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Aggregated Telephony Metadata Is Even More Revealing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mass Collection of Metadata and Data-Mining Across Many Individuals

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

Edward W. Felten

Dated: August 23, 2013

EXHIBIT 1

Edward W. Felten

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

Education

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

Employment

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

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

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

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

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

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

Honors and Awards

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

Research Interests

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

Professional Service

Professional Societies and Advisory Groups

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

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

Program Committees

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

Boards

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

University and Departmental Service

Committee on Online Courses, 2012-present
Director, Center for Information Technology Policy, 2005-present.
Committee on the Course of Study, 2009-present.
SEAS Strategic Planning, 2004.
    Member, Executive Committee
    Co-Chair, Interactions with Industry area.
    Co-Chair, Engineering, Policy, and Society area.
Faculty Advisory Committee on Policy, 2002-present.
Council of the Princeton University Community, 2002-present (Executive Committee)
Faculty Advisory Committee on Athletics, 1998-2000.

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

Students Advised

Ph.D. Advisees:

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

Significant Advisory Role:

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

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

Publications

Books and Book Chapters

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

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

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

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

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

Journal Articles

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

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

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

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

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

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

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

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

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

Selected Symposium Articles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Selected Other Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, NEW YORK CIVIL LIBERTIES UNION, and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

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

Defendants.

Case No. 13-cv-03994 (WHP)

ECF Case

DECLARATION OF MICHAEL GERMAN

I, Michael German, hereby declare and state as follows:

1. I am a resident of the Commonwealth of Virginia over the age of 18 and am principally employed in the District of Columbia. I have personal knowledge of the facts stated in this declaration.

2. I am a Senior Policy Counsel on National Security, Immigration, and Privacy at the American Civil Liberties Union ("ACLU"), where I have worked since 2006. In my work at the ACLU, I am an advocate on issues related to national security and government transparency,

and I am the ACLU's principal advocate on issues related to "whistleblowers," or individuals inside of government who wish to expose government wrongdoing (including illegality, waste, fraud, or abuse) through appropriate and legal channels. I have expertise in this area in part because I am a former federal whistleblower myself.

3. The ACLU is dedicated to defending the rights guaranteed in the Constitution and Bill of Rights, including the free-speech rights of government employees and the public's right to government information produced for public benefit and at public expense. Often, government employees and contractors are the only people in positions to disclose government waste, fraud, abuse, and illegality, and they therefore must be empowered to responsibly report these matters to the appropriate oversight officials within the executive branch—as well as to Congress, the courts and the public—without fear of reprisal. This is particularly true in the national-security context, where inappropriate or excessive use of classification can be used to hide government activities from congressional, judicial, and public oversight, and where the laws protecting whistleblowers from reprisal are weakest.

4. The ACLU lobbies in Congress and directly to executive-branch agencies to strengthen the legal protections for whistleblowers, and to provide effective due-process mechanisms for adjudicating government employees' and contractors' complaints of reprisal for having reporting waste, fraud, abuse, and illegality. The ACLU supported the Whistleblower Protections Enhancement Act of 2012, and encouraged the executive branch to promulgate Presidential Police Directive 19, which is designed to expand protections for employees of the intelligence agencies.

5. Because the ACLU is a prominent organization working on these issues, whistleblowers often contact the ACLU directly, seeking advice, representation, or both.

Because of my background as a whistleblower, many whistleblowers contact me directly to seek my guidance. In these cases, I assist prospective whistleblowers in obtaining legal advice from ACLU litigators or from public-interest groups outside the ACLU, such as the National Whistleblower Center, the Project on Government Oversight, the James Madison Project, and the Government Accountability Project, among others. I may also introduce them to congressional staff, or give them advice on which committees or members of Congress work on the issues they are concerned about or oversee the agencies in which they work. Many times I ask them if they are willing to lose their jobs in the process of bringing a problem to light. If they say "no," I often advise them that the legal protections existing today are insufficient to protect them from retaliation and they should carefully consider their decision. In some cases they do not report the misconduct as a result.

6. I sought assistance from the ACLU when I left the FBI and reported problems in the FBI counterterrorism program to Congress and the public. The ACLU also represented former FBI linguist Sibel Edmunds, who was improperly fired by the FBI after reporting problems in the agency's translation program. The ACLU of Southern California represented Federal Air Marshal Frank Terreri, who was suspended after raising concerns about policy changes that made it easier to identify Federal Air Marshals while on duty protecting air traffic. The ACLU has also assisted many other whistleblowers who have never been publicly identified.

PERSONAL WHISTLEBLOWING HISTORY

7. In June 1988, after graduating from Northwestern University Law School, I entered on duty as a Special Agent at the Federal Bureau of Investigation ("FBI"). During my career at the FBI, I had a clean disciplinary record and a consistent record of superior performance appraisals, and I received a Medal of Valor from the Los Angeles Federal Bar

Association, and a First African Methodist Episcopal Church FAME Award. In addition, through my work as an undercover agent, I successfully infiltrated domestic terrorist organizations, recovered dozens of illegal firearms and explosive devices, successfully investigated unsolved bombings, prevented acts of terrorism, and helped win criminal conviction against terrorists.

8. In 2002, I made a protected disclosure through my chain of command about management failures and violations of law in an FBI counterterrorism investigation. In particular, I learned in August 2002 that part of a meeting between subjects of an FBI investigation in which I was involved had been illegally recorded, in violation of Title III wiretap laws, by an FBI cooperating witness. On September 10, 2002, I sent a letter documenting the illegality of which I was aware up my chain of command. Almost immediately, I suffered retaliation from superior officers; later, I learned that retaliatory investigations, which were shown to be meritless, had been initiated against me because of the misconduct I reported. In November 2002, I reported the entirety of the matter to the Office of the Inspector General ("OIG") in the Department of Justice ("DOJ"). In 2004, I resigned from the FBI as a result of the retaliation I suffered after reporting the misconduct.

9. After two years of attempting to have the misconduct and deficiencies that I witnessed addressed within the FBI and DOJ, I chose to report the matter to Congress. As a result of the efforts of Senators Chuck Grassley, Arlen Specter, and Patrick Leahy, among others, the OIG ultimately released a report documenting the investigation precipitated by the illegality I reported within the FBI. The report confirms many of the allegations in my original complaint. In 2008, I testified before the House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security about my whistleblowing experience within the FBI.

EXPERIENCE WITH WHISTLEBLOWERS AS ACLU POLICY COUNSEL

10. Since joining the ACLU in 2006, I have specialized in advocacy related to federal law enforcement. The primary focus of my work is the role of whistleblowers in exposing government wrongdoing, waste, fraud, and abuse. I estimate that 15 to 25 percent of my professional time is spent on this focus.

11. According to a May 2009 report by the DOJ Office of the Inspector General, *Review of the Federal Bureau of Investigation's Disciplinary System*, a survey of FBI employees indicated that 18 percent of respondents said that they "never" reported incidents of possible misconduct of which they had been made aware. Additionally, 28 percent of respondents in non-supervisory positions (GS-13 grade level or below) indicated that they "never" reported incidents of possible misconduct of which they had been made aware. The report indicated that the second-most-common reason for FBI employees failing to report misconduct incidents was fear of professional retaliation.

12. In my professional capacity, I regularly receive calls from government employees seeking advice on how to "blow the whistle" appropriately, safely, and effectively within different government agencies. In general, my relationships with these individuals are not confined to a single contact, but consist of continuing and ongoing discussions about various attempts to report misconduct and avoid retaliation that may last years at a time. The potential whistleblowers typically do not know their rights under the law, or the proper methods to report waste, fraud, abuse, or illegality within their agencies. They often do not know the responsibilities of the Inspectors General of their agencies, or how to report a complaint to those officials. Finally, they often do not know how they may bring the matter to the attention of members of Congress, and need assistance in identifying the proper committee or member to which they can report their concerns. Even after reporting through these avenues, however,

whistleblowers often need continuing assistance if, for example, the Inspectors General or congressional staff do not properly follow up to investigate the matters. Additionally, after initial reporting, whistleblowers often begin to suffer retaliation as a result of their protected disclosures. I often work with congressional staff and with staff of the Inspector General offices to address the concerns presented by federal whistleblowing.

13. In addition, sometimes individuals within the government contact me about government misconduct but cannot explain themselves fully because doing so would reveal classified information. These individuals usually are seeking safe avenues for communicating and reporting information that may be classified without committing a crime. In my experience, most of these individuals contact me because they are unaware of avenues within the government for reporting misconduct related to classified matters without exposure to adverse retaliation. In my professional experience, less than ten percent of federal-government whistleblowing involves classified information.

14. In most cases, my role in advising potential whistleblowers is to provide guidance about the available avenues for reporting government misconduct, waste, fraud, or abuse, based on my experience and expertise, as well as to assist individuals in retaining legal counsel should the individual desire it.

15. In my experience, government employees who have witnessed possible incidents of misconduct fear that they will suffer professional retaliation if they report those incidents through administrative channels.

16. In the context of whistleblowing, I am aware of various forms of professional retaliation that have occurred in the past and that commonly dissuade individuals from coming forward with information about possible government misconduct, waste, fraud, or abuse. Such

retaliation includes, but is not limited to: harassment; retaliatory investigations; internal disciplinary actions; adverse change of job duties or responsibilities; physical-location transfers; termination; and filing of criminal charges.

17. Additionally, individuals who hold security clearances from the federal government risk losing their clearance status by reporting misconduct. I am aware of numerous cases in which whistleblowers lost security clearances after reporting incidents of misconduct, or had their security clearances threatened. Employees and contractors of the FBI and intelligence agencies have little ability to defend themselves against security-clearance retaliation, and in most cases cannot maintain employment with these agencies without a clearance.

18. In my experience, one of the most dissuasive acts of professional retaliation that potential whistleblowers fear is the threat of administrative investigation. I am aware of numerous instances in which government employees chose not to report misconduct because they feared being subjected to investigations unrelated to the subject of their potential reporting. I have often heard potential whistleblowers express the concern that "no one is administratively pure," which means that no federal employee believes him- or herself to be immune to retaliatory actions if he or she were to report misconduct.

19. Typically, individuals who contact me seeking information about how to safely and legally report government misconduct are fearful that their efforts will be exposed before they decide on a course of action, and are afraid of retaliation that could damage or end their careers. Often, potential whistleblowers are perplexed and frustrated that attempts to report incidents internally are met with resistance and inaction. Many indicate that they believe there are few (and sometimes no) avenues for open communication, advice, or resources about how to

report government misconduct without exposing themselves to adverse employment consequences.

20. When contacted by individuals interested in reporting government misconduct through official channels, I regularly inform them that, based on my personal and professional experiences, simply reporting misconduct commonly leads to dismissal and other serious professional retaliation, and that they must be prepared for those potential consequences.

21. In my experience, most government whistleblowers are dedicated federal employees who have rarely found themselves in a position to challenge the government previously. Not uncommonly, individuals who contact me about potential avenues for whistleblowing are contacting the ACLU for the first time. Many times, such individuals have said to me that contacting me and my employer were actions of "last resort," because they feel that they have nowhere else to turn for guidance.

22. Many of the whistleblowers who contact me expect that their initial report of waste, fraud, abuse, or illegality will be appreciated and addressed appropriately by agency management. They are often shocked to find that they have become targets of retaliation instead, and need to report both the original complaint and a complaint of retaliation outside their agency to an Inspector General to seek protection. Unfortunately, going outside the agencies often intensifies the retaliation, and the Inspectors General are unable, and sometimes unwilling, to protect whistleblowers or properly investigate their allegations. This stage of the whistleblower process is often the most difficult for the individuals that I advise. Whistleblowers are mostly dedicated public servants who expect that the agencies they work for share their interest in serving the public welfare with honesty and integrity, and they are deeply disappointed when they find otherwise. Whistleblowers are also often ostracized by their peers, who fear that

assisting, sympathizing or even just associating with whistleblowers will harm their own careers. Whistleblowers tend to expect that their members of Congress will be interested in their stories, but often they cannot even get congressional staff to meet with them or respond to their emails. The few that do ultimately receive some public recognition for their efforts have likely already lost their jobs or their status within the agencies and, if they are members of the intelligence community, are treated as persona non grata, making them unemployable even by private contractors. Whistleblowers who choose to fight retaliation are often forced to endure years and years of litigation, at great personal expense and with little likelihood of success. These are dedicated public servants who are willing to put themselves at great risk to ensure all government agencies are held to account, but this dedication to the public interest often takes an incredible personal toll.

23. Almost universally, potential whistleblowers seeking advice from me are seeking confidentiality as to both the fact and substance of our communications. Often, individuals will contact me using personal phone numbers or email addresses in order to avoid revealing the fact of conversations with me to colleagues or superior officials within the government. Most potential whistleblowers have already raised their concerns internally, and thus understand that any public advocacy based on their accounts will be easily identified with them and could lead to adverse professional consequences.

24. My role as an advocate on whistleblower issues depends on the use of the telephone to communicate with potential whistleblowers, as opposed to other available mediums, such as email. Many of the people considering whistleblowing are extremely conflicted about the course of action to take because of their desire to serve their country by ensuring that the law is upheld, combined with their personal fears over the consequences of reporting actions that they

believe to be wrong. These conversations are emotional and difficult, and their inherent intimacy often makes them ill-suited to be conducted through electronic means. In addition, because of the sensitivity of the subject matter, most individuals who contact me about becoming a whistleblower seek to avoid creating an electronic record of their concerns and conflicts before they make the ultimate decision to come forward to report what they know.

25. In my opinion, many individuals fear that they will be discovered reaching outside a government agency to seek advice about exposing wrongdoing. These individuals are extraordinarily sensitive to the risks involved in reporting misconduct and the possibility of retaliation should they be identified as whistleblowers. As a result, I estimate that the vast majority of federal-government wrongdoing is not reported, and that most federal employees who have witnessed wrongdoing choose to "suffer in silence" as a result.

JUDGMENTS ABOUT THE EFFECT OF SECTION 215 CALL TRACKING ON THE WILLINGNESS OF FEDERAL WHISTLEBLOWERS TO CONTACT THE ACLU

26. Through news reporting and professional discussions, I am familiar with the U.S. government's bulk collection of telephony metadata under Section 215 of the Patriot Act directed at customers of Verizon Business Network Services ("Verizon").

27. I have personally reviewed a contract between the ACLU and Verizon for telephone services. From my review, I understand that Verizon is the phone-service provider for my Washington, D.C. office phone and for my cellular telephone, which is provided by my employer, the ACLU.

28. Knowledge of the frequency, duration, and timing of calls from government employees to me, or vice versa, would reveal the substance of our relationship because it would indicate that they were considering reporting government misconduct and seeking advice from me and my colleagues about how to legally go about that course of action. A small pattern of

calls between me and a federal employee would lead to a reasonable inference that the individual had knowledge of government wrongdoing, irrespective of whether the content of those calls was known.

29. Because of the professional sensitivity and risks involved for federal employees who are considering becoming whistleblowers, it is my judgment that the Section 215 call-tracking program will cause some individuals to remain silent rather than contact me or the ACLU in order to discuss their options in reporting violations. Knowledge that all of their communications with me or the ACLU are being logged by the government would present a substantial reason for individuals who are undecided about reporting violations but fearful of retaliation from reaching out for advice.

30. As a result, some individuals may decide not to seek advice from me or the ACLU about how to safely and legally report government wrongdoing, and some instances of government wrongdoing will likely go unreported.

31. Without direct contact with whistleblowers, my ability to advocate for greater protections for those who report waste, fraud, abuse, and illegality would be severely hampered. In order to design reforms that protect those conscientious employees and contractor who choose to report government wrongdoing, knowledge of how the system works, or doesn't work, is critical. Since the FBI and intelligence agencies are exempted from the Whistleblower Protection Act, internal executive-branch procedures are the only protection for employees of those agencies. As the agency mechanisms to protect whistleblowers are in a constant state of adjustment, being able to determine which practices provide relief and which create a false promise of security only comes from observing how they work for actual whistleblowers. My work for the ACLU in other national-security fields, including intelligence oversight and

classification reform, would also be severely damaged by whistleblowers' reluctance to contact me. Finally, that reluctance would hamper the ACLU's pursuit of its core missions of protecting individual victims of government misconduct and ensuring that the public receives information about that misconduct from those who have witnessed it.

32. In sum, the Section 215 call-tracking program compromises my ability to gather information and give advice that is relevant and necessary to my role and the ACLU's mission of assisting whistleblowers in safely and legally reporting government misconduct, waste, fraud, or abuse.

* * *

33. Pursuant to 28 U.S.C. § 1746, I hereby declare and state under the penalty of perjury that the foregoing is true and correct.

Date: August 26, 2013

MICHAEL GERMAN

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

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

Defendants.

DECLARATION OF STEVEN R. SHAPIRO

Case No. 13-cv-03994 (WHP)

ECF CASE

DECLARATION OF STEVEN R. SHAPIRO

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

1. I am the Legal Director of the American Civil Liberties Union ("ACLU"), which is a plaintiff in this case. I submit this declaration in support of the plaintiffs' motion for a preliminary injunction. I base this declaration on my personal knowledge and on information provided to me by my staff.

2. For purposes of this declaration, I use "ACLU" to refer to both the American Civil Liberties Union and the American Civil Liberties Union Foundation. The American Civil Liberties Union is a 501(c)(4) nonprofit and nonpartisan organization with approximately 500,000 members nationwide dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil-rights laws. It engages in legislative lobbying, public education, and public advocacy. The American Civil Liberties Union Foundation is a 501(c)(3) organization that provides legal representation free of charge to individuals and groups in civil-rights and civil-liberties cases. It also engages in public education and advocacy.

3. I have served as the ACLU's legal director since 1993. In that capacity, I supervise over 100 lawyers, paralegals, and support personnel who work on a wide range of issues, including—to name just a few—national security, police accountability, reproductive rights, LGBT rights, and immigrants' rights.

4. Given the controversial nature of much of the ACLU's work, the organization has a strong interest in protecting not only the content of our communications with clients, sources, and allies, but often the very fact of those communications. Many of these communications occur by telephone. For example:

- ACLU lawyers frequently place or receive telephone calls from individuals relating to potential legal representation in suits against the federal government. Among others, this includes calls from prospective whistleblowers who wish either to inform the ACLU of government misconduct or to seek legal counsel about their decision to expose that misconduct. These individuals often insist that the very fact of their communication with the ACLU be kept confidential.

- Protecting the confidentiality of a client's identity is also a paramount concern in cases where the client has been granted judicial permission to proceed pseudonymously. In such cases, any disclosure of the client's identity is generally limited by a protective order that is then subject to judicial enforcement.
- In addition, ACLU staff has had numerous conversations over the years with government sources, including members of the executive and legislative branches, in furtherance of the ACLU's advocacy efforts. The ground rules for these discussions can include a promise of confidentiality, which would be breached if it became known that the sources were talking to the ACLU, particularly if the fact or timing of those conversations would reveal the likely subject matter of the communications.
- As a nonpartisan organization, the ACLU forms alliances on discrete issues with other organizations across the ideological spectrum. The terms of the cooperation sometimes include a mutual understanding that the collaboration will be kept confidential.
- Finally, ACLU staff speak by telephone with ACLU members and donors. These conversations relate to the ACLU's work, the relationship that members and donors have with the organization, and other topics.

5. The ACLU can and does take measures to protect the confidentiality of sensitive communications from surveillance by the government or other third parties, including the use of encryption software, when deemed appropriate in the exercise of our professional judgment. Based on conversations with staff, however, my understanding is that current technology does not allow us to shield our telephony metadata from the kind of surveillance at issue here. Thus,

to our knowledge, there is no way to protect the identity of persons communicating by telephone with the ACLU through Verizon, even in circumstances where that information is especially sensitive, so long as the challenged surveillance program continues.

6. Since 2007, the ACLU has received its telephone service from Verizon Business Network Services, Inc. ("Verizon"). As of the filing of this declaration, the ACLU continues to receive its telephone service from Verizon.

7. Prior to the disclosures about the NSA's call-tracking program, the ACLU had no knowledge that its telephony metadata was being acquired and retained for years by the government. The ACLU's agreement with Verizon contains a paragraph that is labeled Customer Consent to Use of Customer Proprietary Network Information ("CPNI"), which defines CPNI to include, among other things, "information relating to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications services Customer purchases from Verizon, as well as related local and toll billing information, made available to Verizon solely by virtue of Customer's relationship with Verizon." That provision further states, "Verizon acknowledges that it has a duty, and Customer has a right, under federal and/or state law to protect the confidentiality of Customer's CPNI." Elsewhere, the ACLU's agreement provides that "Verizon will protect the confidentiality of Customer CPNI in accordance with applicable laws, rules and regulations."

8. The NSA program at issue in this case poses a real threat to the ability of the ACLU to do its work. In my opinion, there is a genuine risk that people who would otherwise speak on the telephone with the ACLU will refrain from doing so if they believe that the government will be able to learn that they have been communicating with us. Given what we

understand about the government's surveillance program, I know of nothing we can do to protect those persons from this risk short of ceasing to speak with them on the telephone.

Steven R. Shapiro

STEVEN R. SHAPIRO

Dated: August 26, 2013

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

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

Defendants.

DECLARATION OF CHRISTOPHER DUNN

Case No. 13-cv-03994 (WHP)

ECF CASE

DECLARATION OF CHRISTOPHER DUNN

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

1. I am the Associate Legal Director of the New York Civil Liberties Union, which is a plaintiff in this case. I submit this declaration in support of the plaintiffs' motion for a preliminary injunction. I base this declaration on my personal knowledge and on information provided to me by NYCLU staff.

2. Founded in 1951 as the New York affiliate of the American Civil Liberties Union ("ACLU"), the New York Civil Liberties Union is a 501(c)(4) non-profit, nonpartisan organization that engages in public education and lobbying with respect to constitutional principles of liberty and equality. The NYCLU has more than 40,000 members throughout New York State. It is incorporated in New York and has its principal place of business in New York City. The New York Civil Liberties Union Foundation is a 501(c)(3) non-profit organization that represents clients in lawsuits seeking to advance civil liberties and civil rights, while also engaging in advocacy and public education around these issues. It is incorporated in Delaware and has its principal place of business in New York City. For purposes of this declaration, I use "NYCLU" to refer to both the New York Civil Liberties Union and the New York Civil Liberties Union Foundation.

3. I have served as the NYCLU's Associate Legal Director since 2002. The NYCLU's legal department has approximately 15 lawyers, paralegals, and support personnel who work on a wide range of issues, including—to name just a few—national security, police accountability, freedom of speech, freedom of religion, voting rights, reproductive rights, race, gender and sexual orientation discrimination. The NYCLU frequently co-counsels with the ACLU in national security cases brought in the Southern District of New York. *See, e.g.*, *Clapper v. Amnesty*, 133 S. Ct. 1138 (2013); *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2009).

4. I am familiar with the declaration being filed in this matter by ACLU Legal Director Steven Shapiro. Given the overlap of the work of the NYCLU and ACLU, many of the concerns expressed by Mr. Shapiro on behalf of the ACLU are shared by the NYCLU.

5. NYCLU legal staff frequently place or receive telephone calls from individuals relating to potential legal representation in suits against state and local governments and sometimes against the federal government. Often, the mere fact that the NYCLU has communicated with these individuals is sensitive. For example, the NYCLU has received calls from employees of the New York City Police Department ("NYPD") who wished to inform the NYCLU of misconduct within the NYPD. In virtually all of those calls, police employees have insisted that the very fact of their speaking with the NYCLU be kept strictly confidential.

6. NYCLU legal staff often speak on the telephone to communicate with government and industry whistleblowers, legislators and their staffs, and possible litigation or advocacy partners who consider the confidentiality of their associations and communications with the NYCLU essential to their willingness to speak with us. From time to time, NYCLU staff also speak by telephone with the organization's members.

7. The NYCLU was a customer of Verizon Business Network Services ("Verizon") until early April 2013. Until then, Verizon provided the NYCLU's wired communications, including its landlines.

8. Prior to the disclosures about the NSA mass call-tracking program, the NYCLU believed that its telephone communications through Verizon were secure from routine government monitoring.

9. The NSA program at issue in this case poses a substantial threat to the ability of the NYCLU to do its work, which includes public advocacy on controversial subjects, the representation of clients in litigation or in anticipation of litigation, and efforts to lobby elected local, state, and federal officials. I am confident that there are persons who speak on the

telephone with our legal staff who will refrain from doing so if they believe that the government will be able to learn of the fact that they have communicated with us. The privacy of such communication is clearly compromised by the government's mass call-tracking program. The preliminary injunctive relief requested in this motion is necessary to restore a sense of comfort and confidence in the confidentiality of the various sensitive telephonic communications that we undertake.

CHRISTOPHER DUNN

Dated: August 26, 2013
New York, N.Y.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION, Plaintiffs, v. JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation, Defendants.	**DECLARATION OF PATRICK TOOMEY** Case No. 13-cv-03994 (WHP) **ECF CASE**

DECLARATION OF PATRICK TOOMEY

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

1. I am a resident of Brooklyn, New York, over the age of 18. I have personal knowledge of the facts stated in this declaration.

2. I am an attorney for the American Civil Liberties Union and counsel to the plaintiffs in this action. I submit this declaration in support of Plaintiffs' Motion for Preliminary Injunction.

3. Attached hereto as **Exhibit 1** is a true and correct copy of the Primary Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 13-80 (FISA Ct. Apr. 25, 2013). The Primary Order was declassified by the Director of National Intelligence, James R. Clapper, on July 31, 2013. *See* Office of the Dir. of Nat'l Intelligence, *DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents* (July 31, 2013), http://1.usa.gov/1bJxued.

4. Attached hereto as **Exhibit 2** is a true and correct copy of the Secondary Order, *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISA Ct. Apr. 25, 2013). The Secondary Order was acknowledged as authentic by the Director of National Intelligence, James R. Clapper, on June 6, 2013. *See* Office of the Dir. of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosures of Classified Information* (June 6, 2013), http://1.usa.gov/13jwuFc.

* * *

I declare under penalty of perjury under the laws of the United States and of the State of New York that the forgoing is true and correct.

Patrick C. Toomey

PATRICK TOOMEY

Dated: August 26, 2013
New York, New York

EXHIBIT 1

~~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 [redacted]

Docket Number: BR

13-80

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [redacted] and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production 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"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "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.

~~TOP SECRET//SI//NOFORN~~

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 [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

[redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

~~TOP SECRET//SI//NOFORN~~

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[redacted]

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [redacted], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure, through adequate and

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

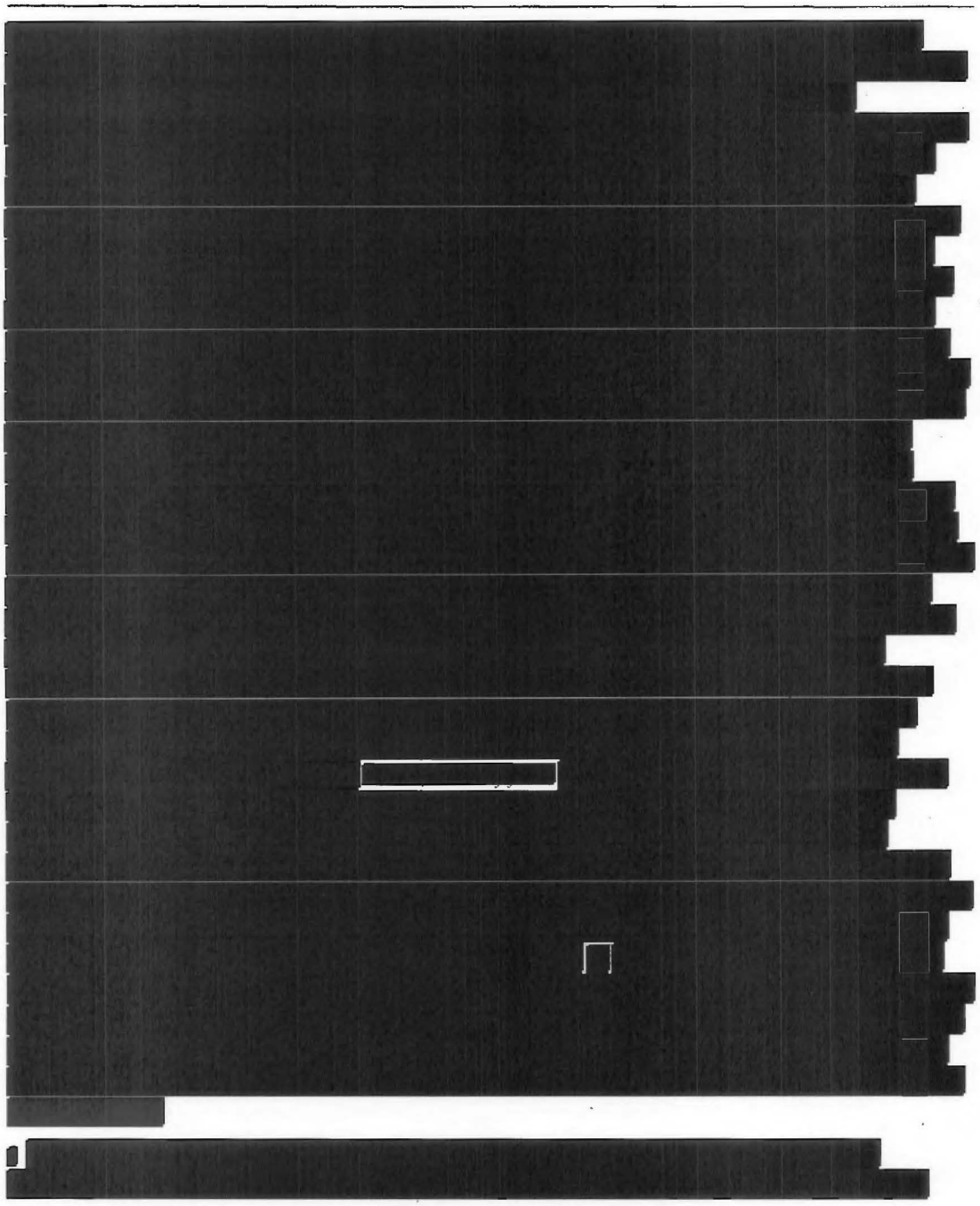
(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

[redacted] provided, however, that NSA's Office of General Counsel (OGC)



~~TOP SECRET//SI//NOFORN~~

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

~~TOP SECRET//SI//NOFORN~~

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

---

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[redacted]

~~TOP SECRET//SI//NOFORN~~

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[redacted]

[11] This automated query process was initially approved by this Court in its [redacted] 2012 Order amending docket number [redacted]

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

~~TOP SECRET//SI//NOFORN~~

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

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

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

EXHIBIT 2

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 13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

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

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

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

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

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

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

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

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

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

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs,

v.

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

Defendants.

13 Civ. 3994 (WHP)

ECF Case

Notice of Motion

PLEASE TAKE NOTICE that upon the accompanying memorandum of law in support of defendants' motion to dismiss the complaint, dated August 26, 2013, and the exhibits thereto, defendants James R. Clapper, in his official capacity as Director of National Intelligence; Keith B. Alexander, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; Charles T. Hagel, in his official capacity as Secretary of Defense; Eric H. Holder, in his official capacity as Attorney General of the United States; and Robert S. Mueller, in his official capacity as Director of the Federal Bureau of Investigation, will move this Court, before the Honorable William J. Pauley, at the United States Courthouse, 500 Pearl Street,

New York, New York, for an Order dismissing the complaint pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure.

PLEASE TAKE FURTHER NOTICE that pursuant to the Court's Corrected Scheduling Order dated August 8, 2013, opposition papers, if any, are to be served on or before September 26, 2013.

Dated: New York, New York
August 26, 2013

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director

ANTHONY J. COPPOLINO
Deputy Director

By: /s/ James Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

Civil Division,
Federal Programs Branch
U.S. Department of Justice
20 Massachusetts Avenue, N.W.
Washington, DC 20001
Tel.: (202) 514-3358

PREET BHARARA
United States Attorney for the
Southern District of New York
Attorney for Defendants

By: /s/ David S. Jones
DAVID S. JONES
TARA M. La MORTE
JOHN D. CLOPPER
CHRISTOPHER HARWOOD
Assistant United States Attorneys
86 Chambers Street, 3rd Floor
New York, New York 10007
Tel. (212) 637-2739/2746/2716/2728
Fax (212) 637-2730
david.jones6@usdoj.gov
tara.lamorte2@usdoj.gov
john.clopper@usdoj.gov
christopher.harwood@usdoj.gov

Exhibit 1

~~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

13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

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

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

~~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~~

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~~

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

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

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

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

Exhibit 2

~~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 [redacted]

Docket Number: BR

13-80

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

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

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [redacted] and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production 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"[1] created by [redacted]

B. The Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

[1] For purposes of this Order "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.

~~TOP SECRET//SI//NOFORN~~

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 [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.[2] The BR metadata shall carry unique markings such

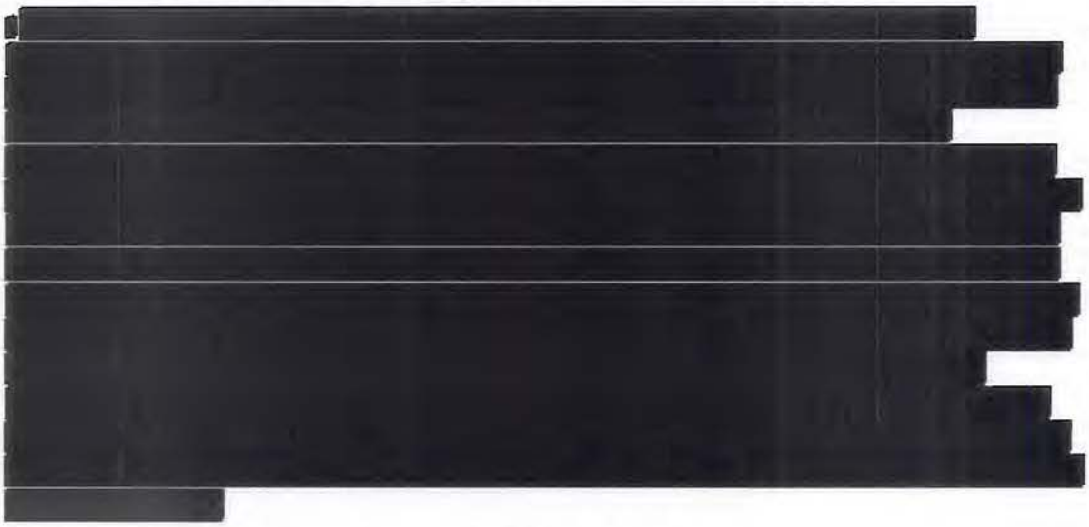
[2] The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.[3] Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms[4] that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

[3] The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.



but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [redacted], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure, through adequate and

[5] For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.[6]

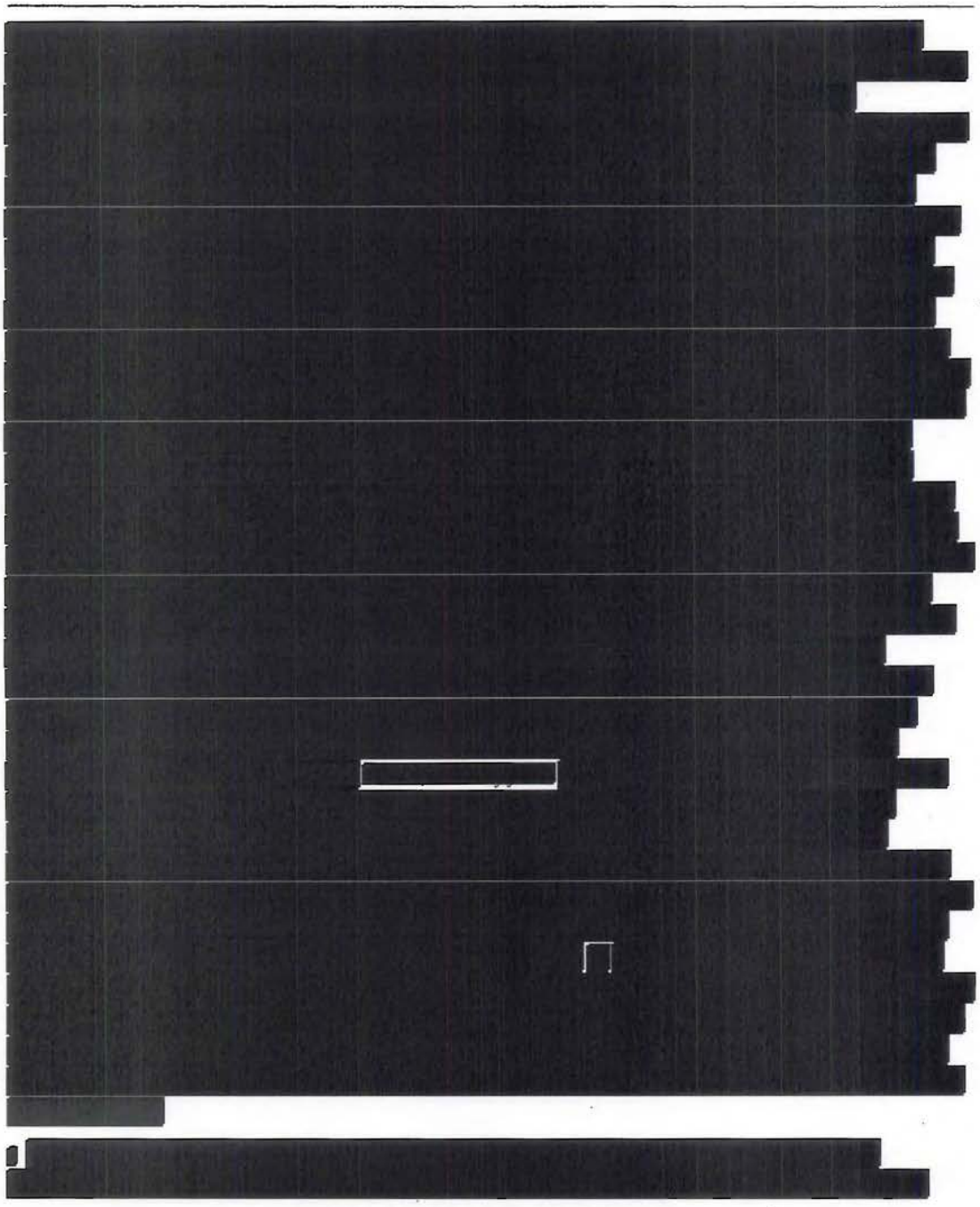
(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [redacted]

[redacted]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

[redacted] provided, however, that NSA's Office of General Counsel (OGC)



~~TOP SECRET//SI//NOFORN~~

shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [redacted] on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [redacted] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[redacted]

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [redacted] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.[9,10]

[9] The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [redacted] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[redacted]

~~TOP SECRET//SI//NOFORN~~

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.[11] This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [redacted] Declaration, are as follows:

[11] This automated query process was initially approved by this Court in its [redacted] 2012 Order amending docket number [redacted]

[12] As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

~~TOP SECRET//SI//NOFORN~~

[redacted]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[redacted]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (i.e., the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.[16] Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

---

[15] In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

[16] In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.[17] OGC shall provide NSD/DoJ with copies

[17] The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

~~TOP SECRET//SI//NOFORN~~

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand

~~TOP SECRET//SI//NOFORN~~

counterterrorism information or to assess its importance.

This authorization regarding [redacted] expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

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

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

Exhibit 3

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 4

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

December 14, 2009

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence
United States House of Representatives
HVC-304, The Capitol
Washington, DC 20515

Dear Chairman Reyes:

~~(TS)~~ Thank you for your letter of September 30, 2009, requesting that the Department of Justice provide a document to the House Permanent Select Committee on Intelligence (HPSCI) that describes the bulk collection program conducted under Section 215 -- the "business records" provision of the Foreign Intelligence Surveillance Act (FISA). We agree that it is important that all Members of Congress have access to information about this program, as well as a similar bulk collection program conducted under the pen register/trap and trace authority of FISA, when considering reauthorization of the expiring USA PATRIOT Act provisions.

~~(TS)~~ The Department has therefore worked with the Intelligence Community to prepare the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States. We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215 and any changes to the FISA pen register/trap and trace authority. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to strict rules.

~~Classified by: Assistant Attorney General, NSD~~
Reason: 1.4(c)
~~Declassify on: 11 December 2034~~

~~TOP SECRET//COMINT//NOFORN~~

~~(TS)~~ Therefore, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) Thank you again for your letter, and we look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,

Ronald Weich
Assistant Attorney General

Exhibit 5

~~TOP SECRET//COMINT//NOFORN~~

~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- ~~(TS//SI//NF)~~ Provisions of the USA PATRIOT Act affected by reauthorization legislation support two sensitive intelligence collection programs;
- ~~(TS//SI//NF)~~ These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by anyone in the government, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the Foreign Intelligence Surveillance Court ("FISA Court") and Congress;
- ~~(TS//SI//NF)~~ The Executive Branch, including DOJ, ODNI, and NSA, takes any compliance problems in the programs very seriously, and substantial progress has been made in addressing those problems. [redacted] and
- ~~(TS//SI//NF)~~ NSA's bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Classified by: Assistant Attorney General, NSD~~
Reason: 1.4(c)
Declassify on: ~~11 December~~ 2034

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the National Security Agency (NSA) intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

> *"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."*

~~(TS//SI//NF)~~ Today, under Foreign Intelligence Surveillance Court authorization pursuant to the "business records" authority of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorism target overseas. This and similar programs operated pursuant to FISA provide valuable intelligence information.

(U) USA PATRIOT Act reauthorization legislation currently pending in both the House and the Senate would alter, among other things, language in two parts of FISA: Section 215 and the FISA "pen register/trap and trace" (or "pen-trap") authority. Absent legislation, Section 215 will expire on December 31, 2009, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The FISA pen-trap authority does not expire, but the pending legislation in the Senate and House includes amendments of this provision.

~~(TS//SI//NF)~~ The Section 215 and pen-trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant uses of these authorities are to support two critical and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from telecommunications providers [redacted] Although these programs have been briefed to

the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [redacted] telecommunications companies [redacted] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen-trap provisions in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as "to" and "from" lines in e-mail and the time an e-mail is sent – excluding the content of the e-mail and the "subject" line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment. [redacted]

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [redacted]

~~TOP SECRET//COMINT//NOFORN~~

Checks and Balances

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen-trap provision. Before obtaining any information from a telecommunication service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before an NSA analyst may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [redacted] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [redacted] is provided to NSA personnel for further intelligence analysis. There are also limits on how long the collected data can be retained (5 years in the Section 215 program, and 4½ years in the pen-trap program).

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, to include hearings, briefings, and, with respect to the Intelligence Committees, visits to NSA. In addition, the Intelligence Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ There have been a number of technical compliance problems and human implementation errors in these two bulk collection programs, discovered as a result of Department of Justice reviews and internal NSA oversight. However, neither the Department, NSA nor the FISA Court has found any intentional or bad-faith violations. The problems generally involved the implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the Court's orders. In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered "end-to-end" reviews of the Section 215 and pen-trap collection programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection. In early September of 2009, the Director of NSA made a presentation to the FISA Court about the steps taken to address the compliance issues. All

parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify the network of contacts that a targeted number or address is connected to, whenever there is RAS that the number or address is associated with [redacted] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata. (Communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content.). The more metadata NSA has access to, the more likely it is that NSA can identify or discover the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

****

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen-trap bulk collection programs provide a vital capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

Exhibit 6

United States Senate

SELECT COMMITTEE ON INTELLIGENCE

WASHINGTON, DC 20510–6475

February 23, 2010

Dear Colleague:

Three provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA) will sunset on February 28, 2010: (1) authority for roving electronic surveillance of targets who take steps to thwart FISA surveillance (Section 206 of the USA PATRIOT Act); (2) authority to compel production of business records and other tangible things with the approval of the FISA Court (Section 215 of the USA PATRIOT Act); and (3) authority to target non-U.S. person "lone wolves" who engage in international terrorist activities but are not necessarily associated with an identified terrorist group (Section 6001 of the Intelligence Reform and Terrorism Prevention Act).

Members of the Select Committee on Intelligence have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of intelligence authority on which they are asked to vote. In response to these requests, the Attorney General and the Director of National Intelligence have provided a classified paper to the House and Senate Intelligence Committees on important intelligence collection made possible by authority that is subject to the approaching sunset, and asked for our assistance in making it available, in a secure setting, directly and personally to any interested Member.

We would like to invite each Member of the Senate to read this classified paper in the Intelligence Committee's offices in 211 Hart Senate Office Building. The Attorney General and DNI have offered to make Department of Justice and Intelligence Community personnel available to meet with any Member who has questions. We will be pleased to make members of our staff available for the same purpose. Please contact our Security Director, James Wolfe, at 224-1751, to arrange for a time.

Sincerely,

Dianne Feinstein
Chairman

Christopher S. Bond
Vice Chairman

Exhibit 7

USA Patriot Act

From: The Permanent Select Committee on Intelligence
Sent By: Khizer.Syed@mail.house.gov
Date: 2/25/2010

February 24, 2010

Dear Colleague:

Three provisions of the USA PATRIOT Act are set to expire on February 28, 2010: (1) authority for roving electronic surveillance of targets who take steps to thwart FISA surveillance; (2) authority to compel production of business records and other tangible things with the approval of the FISA Court; and (3) authority to target non-U.S. person "lone wolves" who engage in international terrorist activities, but are not necessarily associated with an identified terrorist group.

In advance of the anticipated House consideration of a one-year extension of the three provisions described above, the Attorney General and the Director of National Intelligence have provided a classified document to the congressional intelligence committees on important intelligence collection programs made possible by these expiring authorities. They have asked for the Committee's assistance in making that document available to interested members of Congress.

I have agreed to accommodate this request, and Chairman Conyers and I will make Judiciary and Intelligence Committee staff available to meet with any member who has questions. The Attorney General and DNI will also make Department of Justice and Intelligence Community personnel available if needed.

If you are interested in reviewing this classified document, please contact the Committee's scheduler, Stephanie Leaman, at x57690, to set up an appointment in the Committee offices, located in HVC-304.

Sincerely,

/s/

Silvestre Reyes
Chairman
Permanent Select Committee on Intelligence

Exhibit 8

~~TOP SECRET//COMINT//NOFORN~~

~~(TS//SI//NF)~~ Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- (U) Section 215 of the USA PATRIOT Act, which expires at the end of February 2011, allows the government, upon approval of the Foreign Intelligence Surveillance Court ("FISA Court"), to obtain access to certain business records for national security investigations;
- (U) Section 402 of the Foreign Intelligence Surveillance Act ("FISA"), which is not subject to a sunset, allows the government, upon approval of the FISA Court, to install and use a pen register or trap and trace ("pen/trap") device for national security investigations;
- ~~(TS//SI//NF)~~ These authorities support two sensitive and important intelligence collection programs. These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress;
- ~~(TS//SI//NF)~~ Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court; and
- ~~(TS//SI//NF)~~ The National Security Agency's (NSA) bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20360101~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

Background

~~(TS//SI//NF)~~ Since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the NSA intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating the location from where al-Mihdhar was calling. Lacking the originating phone number, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

> *"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."*

~~(TS//SI//NF)~~ Today, under FISA Court authorization pursuant to the "business records" authority of the FISA (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorist overseas. This and similar programs operated pursuant to FISA, including exercise of pen/trap authorities, provide valuable intelligence information.

(U) Absent legislation, Section 215 will expire on February 28, 2011, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The pen/trap authority does not expire.

~~(TS//SI//NF)~~ The Section 215 and pen/trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant use of these authorities is to support two important and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States. [redacted] Although these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring

PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

Section 215 and Pen-Trap Collection

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from certain telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [redacted] telecommunications companies [redacted] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen/trap provision in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as "to" and "from" lines in e-mail, certain routing information, and the date and time an e-mail is sent – excluding the content of the e-mail and the "subject" line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment.

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [redacted] However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.

Checks and Balances

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen/trap provision. Before obtaining any information from a telecommunications service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before NSA analysts may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [redacted]

~~TOP SECRET//COMINT//NOFORN~~

[redacted] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [redacted] is provided to NSA personnel for further intelligence analysis. The bulk data collected under each program can be retained for 5 years.

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, through hearings, briefings, and visits to NSA. In addition, the Intelligence and Judiciary Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ In 2009, a number of technical compliance problems and human implementation errors in these two bulk collection programs were discovered as a result of Department of Justice (DOJ) reviews and internal NSA oversight. However, neither DOJ, NSA, nor the FISA Court has found any intentional or bad-faith violations. [redacted] In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The FISA Court placed several restrictions on aspects of the business records collection program until the compliance processes were improved to its satisfaction. [redacted]

(U) The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed safeguards that, together with greater efforts by the Executive Branch, have resulted in significant and effective changes in the compliance program.

(U) All parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

Intelligence Value of the Collection

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States that may be contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and entirely domestic connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify and assess the network of contacts that a targeted number or address is connected to, whenever there is RAS that the targeted number or address is associated with [redacted] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata – but always based on links to a number or e-mail address which itself is associated with a counterterrorism target. (Again, communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content) The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

****

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen/trap bulk collection programs provide an important capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.

Exhibit 9

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Dianne Feinstein
Chairman
The Honorable Saxby Chambliss
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Madam Chairman and Mr. Vice Chairman:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the SSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the SSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~
Reason: 1.4(c)
~~Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that SSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the House Permanent Select Committee on Intelligence (HPSCI) under similar conditions, so that it may be made available to the Members of the House, as well as cleared leadership, HPSCI and House Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 10

~~TOP SECRET//COMINT//NOFORN~~

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Mike Rogers
Chairman
The Honorable C.A. Dutch Ruppersberger
Ranking Minority Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Congressman Ruppersberger:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~
Reason: 1.4(c)
~~Declassify on: February 2, 2036~~

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT//NOFORN~~

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

~~TOP SECRET//COMINT//NOFORN~~

Exhibit 11

SSCI# 2011 - 0823

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-6475

February 8, 2011

Dear Colleague:

Three provisions of the Foreign Intelligence Surveillance Act of 1978 (FISA) will sunset on February 28, 2011. Two – one on roving authority for electronic surveillance and the other on the acquisition of business records that are relevant to investigations to protect against international terrorism or espionage – were added to FISA by the USA PATRIOT Act. The third, on "lone wolf" authority under FISA, was added by the Intelligence Reform Act of 2004.

Members of our Committee have previously requested that the Executive Branch permit each Member of Congress access to information on the nature and significance of the intelligence authority on which they are asked to vote. In response, last year the Attorney General and the Director of National Intelligence (DNI) provided a classified report to the House and Senate Intelligence Committees in advance of the previous sunset date of February 28, 2010. At the request of our Committee, the Attorney General and DNI have now provided an updated classified report for review by Members in connection with this year's February 28, 2011 sunset. As was requested last year, they have asked that any interested Member review this report in a secure setting.

We invite each Senator to read this classified report in our committee spaces in Room 211, Hart Senate Office Building. The Attorney General and DNI have offered to make Justice Department and Intelligence Community personnel available to meet with any Member who has questions. We will be pleased to make our staff available for the same purpose. Please contact our Security Director, James Wolfe, at 224-1751, to arrange to read the report.

Sincerely,

Dianne Feinstein
Chairman

Saxby Chambliss
Vice Chairman

Exhibit 12

Press Release of Intelligence Committee

Feinstein, Chambliss Statement on NSA Phone Records Program

Contact: Brian Weiss (Feinstein), (202) 224-9629
Lauren Claffey (Chambliss), (202) 224-3423

Thursday, June 6, 2013

Washington—Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) and Vice Chairman Saxby Chambliss (R-Ga.) today released the following joint statement:

"A primary mission of the U.S. intelligence community is to detect and prevent terrorist attacks against the United States, and Congress works closely with the executive branch to ensure that the authorities necessary to keep our country safe are in place. One of these authorities is the 'business records' provision of the Foreign Intelligence Surveillance Act under which the executive branch is authorized to collect 'metadata' concerning telephone calls, such as a telephone number or the length of a call. This law does not allow the government to listen in on the content of a phone call.

"The executive branch's use of this authority has been briefed extensively to the Senate and House Intelligence and Judiciary Committees, and detailed information has been made available to all members of Congress prior to each congressional reauthorization of this law.

"Ensuring security, however, must be consistent with respect for the constitutional rights of all Americans. The alleged FISA Court order contained in the *Guardian* article does not give the government authority to listen in on anyone's telephone call, nor does it provide the government with the content of any communication or the name of any subscriber. As with other FISA authorities, all information the government may receive under such an order would be subject to strict limitations. While our courts have consistently recognized that there is no reasonable expectation of privacy in this type of metadata information and thus no search warrant is required to obtain it, any subsequent effort to obtain the content of an American's communications would require a specific order from the FISA Court.

"The intelligence community has successfully used FISA authorities to identify terrorists and those with whom they communicate, and this intelligence has helped protect the nation. The threat from terrorism remains very real and these lawful intelligence activities must continue, with the careful oversight of the executive, legislative and judicial branches of government."

###

Search

211 Hart Senate Office Building, Washington, D.C. 20510 Phone: 202-224-1700

Exhibit 13

Title Info

Title:
REP. MIKE D. ROGERS HOLDS A HEARING ON SURVEILLANCE PROGRAMS

Date:
June 18, 2013

Location:
WASHINGTON, D.C.

Committee:
Permanent Select Committee on Intelligence. House

Permalink:
HTTP://congressional.proquest.com/congressional/docview/t65.d40.06180003.u30?accountid=14740

Speaker

REP. MIKE D. ROGERS

Body

ROGERS: The committee will come to order.

General Alexander, Deputy Attorney General Cole, Chris Inglis, Deputy Director Joyce and Mr. Litt, thank you for appearing before us today, especially on short notice.

The ranking member and I believe it is important to hold an open hearing today, and we don't do a tremendous amount of those, to provide this House and the public with an opportunity to hear directly from you how the government is using the legal authorities that Congress has provided to the executive branch since the terrorist attacks of September 11th, 2001.

I'd also like to recognize the hard work of the men and women of the NSA and the rest of the intelligence community who work day in and day out to disrupt threats to our national security. People at the NSA in particular have heard a constant public drumbeat about a laundry list of nefarious things they are alleged to be doing to spy on Americans -- all of them wrong. The misperceptions have been great, yet they keep their heads down and keep working every day to keep us safe.

ROGERS: And, General Alexander, please convey our thanks to your team for continuing every day, despite much misinformation about the quality of their work. And thank them for all of us for continuing to work to protect America.

I also want to take this moment to thank General Alexander who has been extended as national security adviser in one way or another three different times. That's a patriot.

This is a very difficult job at a very difficult time in our history. And for the general to accept those extensions of his military service to protect this nation, I think with all of the -- the, again, the misinformation out there, I want to thank you for that.

Thank you for your patriotism. Thank you for continuing to serve to protect the United States, again. And you have that great burden of knowing lots of classified information you cannot talk publicly about. I want you to know, thank you on behalf of America for your service to your country.

The committee has been extensively briefed on these efforts over a regular basis as a part of our ongoing oversight responsibility over the 16 elements of the intelligence community and the national intelligence program.

In order to fully understand the intelligence collection programs most of these briefings and hearings have taken place in classified settings. Nonetheless, the collection efforts under the business records provision in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and subject to an extensive oversight regime.

I look forward from hearing from all of the witnesses about the extensive protections and oversight in place for these programs.

General Alexander, we look forward to hearing what you're able to discuss in an open forum about how the data that you have -- you obtain from providers under court order, especially under the business records provision, is used.

And Deputy Attorney General Cole, we look forward to hearing more about the legal authorities themselves and the state of law on what privacy protections Americans have in these business records.

One of the frustrating parts about being a member of this committee, and really challenge, is sitting at the intersection of classified intelligence programs and transparent democracy as representatives of the American people.

The public trusts the government to protect the country from another 9/11-type attack, but that trust can start to wane when they are faced with inaccuracies, half truths and outright lies about the way the intelligence programs are being run.

One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government.

This is particularly so when those of us who have taken the oath to protect information that can damage the national security if released cannot publicly provide clarifying information because it remains classified.

It is at times like these where our enemies with -- our enemies within become almost as damaging as our enemies on the outside.

It is critically important to protect sources and methods so we aren't giving the enemy our play book.

It's also important, however, to be able to talk about how these

programs help protect us so they can continue to be reauthorized. And then we highlight the protections and oversight of which these programs operate under.

General Alexander, you and I have talked over the last week, about the need to -- to be able to publicly elaborate on the success stories these authorities have contributed to without jeopardizing ongoing operations. I know you'll have the opportunity to talk about several of those today.

I place the utmost value in protecting sources and methods. And that's why you've been, I think, so diligent in making sure that anything that's disclosed comports with the need to protect sources and methods. So that, again, we don't make it easier for the bad guys overseas, terrorists in this case, to do harm to United States citizens, and I respect that.

I also recognize that when we are forced into the position of having so publicly discussed intelligence programs due to irresponsible criminal behavior that we also have to be careful to balance the need for secrecy while educating the public.

I think you have struck the right balance between protecting sources and methods and maintaining the public's trust by providing more examples of how these authorities have helped disrupt terrorist plots and connections. I appreciate your efforts in this regard.

For these authorities to continue, they must continue to be available. Without them, I fear we will return to the position where we were prior to the attacks of September 11th, 2001. And that would be unacceptable for all of us.
I hope today's hearing will help answer questions that have arisen as a result of the fragmentary and distorted illegal disclosures over the past several days.

Before recognizing General Alexander for his opening statement, I turn the floor over to the ranking member for any opening statement he'd like to make.

RUPPERSBERGER: Well, I agree with really a lot of what the chairman said.

General Alexander, Chris Inglis, you know, your leadership in NSA has been outstanding. And I just want to acknowledge the people who work at NSA every day. NSA is in my district. I have an occasion to communicate, and a lot of the people who go to work to protect our country, who work hard every day, are concerned that the public think they're doing something wrong. And that's not the case at all.

And the most important thing we can do here today is let the public know the true facts. I know that Chairman Rogers and I and other members have asked you to help declassify what we can, that will not hurt our security, so the public can understand that this important (sic) is legal, why we're doing this program and how it protects us.

We're here today because of the brazen disclosure of critical

classified information that keeps our country safe. This widespread leak by a 29-year-old American systems administrator put our country and our allies in danger by giving the terrorists a really good look at the play book that we use to protect our country. The terrorists now know many of our sources and methods.

There's been a lot in the media about this situation. Some right. A lot wrong. We're holding this open hearing today so we can set the record straight and the American people can hear directly from the intelligence community as to what is allowed and what is not under the law. We need to educate members of Congress also, with the public.

To be clear, the National Security Agency is prohibited from listening in on phone calls of Americans without proper, court-approved legal authorities.

We live in a country of laws. These laws are strictly followed and layered with oversight from three branches of government, including the executive branch, the courts and Congress.

Immediately after 9/11, we learned that a group of terrorists were living in the United States actively plotting to kill Americans on our own soil. But we didn't have the proper authorities in place to stop them before they could kill almost 3,000 innocent people.

Good intelligence is clearly the best defense against terrorism. There are two main authorities that have been highlighted in the press, the business records provision that allows the government to legally collect what is called metadata, simply the phone number and length of call. No content, no conversations. This authority allows our counterterrorism and the law enforcement officials to close the gap on foreign and domestic terrorist activities. It enables our intelligence community to discover whether foreign terrorists have been in contact with people in the U.S. who may be planning a terrorist attack on U.S. soil.

The second authority is known as Section 702 of the FISA Amendment Act. It allows the government to collect the content of e-mail and phone calls of foreigners -- not Americans -- located outside the United States. This allows the government to get information about terrorists, cyber-threats, weapons of mass destruction and nuclear weapons proliferation that threaten America.

This authority prohibits the targeting of American citizens or U.S. permanent residents without a court order, no matter where they are located.

Both of these authorities are legal. Congress approved and reauthorized both of them over the last two years. In fact, these authorities have been instrumental in helping prevent dozens of terrorist attacks, many on U.S. soil.

But the fact still remains that we must figure out how this could have happened. How was this 29-year-old systems administrator able to access such highly classified information and about such sensitive matters? And how was he able to download it and remove it from his

workplace undetected?

We need to change our systems and practices, and employ the latest in technology that would alert superiors when a worker tries to download and remove this type of information. We need to seal this crack in the system.

And to repeat something incredibly important: The NSA is prohibited from listening to phone calls or reading e-mails of Americans without a court order. Period. End of story.

Look forward your testimony.

ROGERS: Again, thank you very much.

Thanks, Dutch, for that.

General Alexander, the floor is yours.

ALEXANDER: Chairman, Ranking Member, thank you for the kind words. I will tell you it is a privilege and honor to serve as the director of the National Security Agency and the commander of the U.S. Cyber Command.

As you noted, we have extraordinary people doing great work to protect this country and to protect our civil liberties and privacy.

Over the past few weeks, unauthorized disclosures of classified information have resulted in considerable debate in the press about these two programs.
The debate had been fueled, as you noted, by incomplete and inaccurate information, with little context provided on the purpose of these programs, their value to our national security and that of our allies, and the protections that are in place to preserve our privacy and civil liberties.

Today, we will provide additional detail and context on these two programs to help inform that debate.

These programs were approved by the administration, Congress and the courts. From my perspective, a sound legal process that we all work together as a government to protect our nation and our civil liberties and privacy.

ALEXANDER: Ironically, the documents that have been released so far show the rigorous oversight and compliance our government uses to balance security with civil liberties and privacy.

Let me start by saying that I would much rather be here today debating this point than trying to explain how we failed to prevent another 9/11. It is a testament to the ongoing team work of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, working with our allies and industry partners, that we have been able to connect the dots and prevent more terrorist attacks.

The events of September 11, 2001 occurred, in part, because of a failure on the part of our government to connect those dots. Some of those dots were in the United States. The intelligence community was not able to connect those domestic dots, phone calls between operatives and the U.S. and Al Qaida terrorist overseas. Following the 9/11 commission, which investigated the intelligence community's failure to detect 9/11, Congress passed the PATRIOT Act.

Section 215 of that act, as it has been interpreted and implied, helps the government close that gap by enabling the detection of telephone contact between terrorists overseas and operatives within the United States. As Director Mueller emphasized last week during his testimony to the -- to the Judiciary Committee, if we had had Section 215 in place prior to 9/11, we may have known that the 9/11 hijacker Mihdhar was located in San Diego and communicating with a known Al Qaida safe house in Yemen.

In recent years, these programs, together with other intelligence, have protected the U.S. and our allies from terrorist threats across the globe to include helping prevent the terrorist -- the potential terrorist events over 50 times since 9/11. We will actually bring forward to the committee tomorrow documents that the interagency has agreed on, that in a classified setting, gives every one of those cases for your review. We'll add two more today publicly we'll discuss. But as the chairman noted, if we give all of those out, we give all the secrets of how we're tracking down the terrorist as a community. And we can't do that. Too much is at risk for us and for our allies. I'll go into greater detail as we go through this testimony this morning.

I believe we have achieved the security and relative safety in a way that does not compromise the privacy and civil liberties of our citizens. We would like to make three fundamental points. First, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community efforts to connect the dots.

Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes in oversight mechanisms. We have rigorous train programs for our analysts and their supervisors to understand their responsibilities regarding compliance.

Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people. We will provide important details about each of those. First, I'd -- I'd ask the Deputy Attorney General Jim Cole to discuss the overarching framework of our authority.

Sir.

COLE: Thank you -- thank you, General.

Mr. Chairman, Mr. Ranking Member, members of the committee, as General Alexander said, and -- and as the chairman and ranking member have said, all of us in the national security area are constantly trying to balance protecting public safety with protecting people's

privacy and civil liberties in this government. And it's a constant job at balancing this.

We think we've done this in these instances. There are statutes that are passed by Congress. This -- this is not a program that's off the books, that's been hidden away. This is part of what government puts together and discusses. Statutes are passed. It is overseen by three branches of our government, the Legislature, the Judiciary, and the Executive Branch. The process of oversight occurs before, during, and after the processes that we're talking about today.

And I want to talk a little bit how that works, what the legal framework is, and what some of the protections are that are put into it. First of all, what we have seen published in the newspaper concerning 215 -- this is the business records provisions of the PATRIOT Act that also modify FISA.

You've seen one order in the newspaper that's a couple of pages long that just says under that order, we're allowed to acquire metadata, telephone records. That's one of two orders. It's the smallest of the two orders. And the other order, which has not been published, goes into, in great detail; what we can do with that metadata; how we can access it; how we can look through it; what we can do with it, once we have looked through it; and what the conditions are that are placed on us to make sure that we protect privacy and civil liberties; and, at the same time, protect public safety.

Let me go through a few of the features of this. First of all, it's metadata. These are phone records. These -- this is just like what you would get in your own phone bill. It is the number that was dialed from, the number that was dialed to, the date and the length of time. That's all we get under 215. We do not get the identity of any of the parties to this phone call. We don't get any cell site or location information as to where any of these phones were located. And, most importantly, and you're probably going to hear this about 100 times today, we don't get any content under this. We don't listen in on anybody's calls under this program at all.

This is under, as I said, section 215 of the PATRIOT Act. This has been debated and up for reauthorization, and reauthorized twice by the United States Congress since its inception in 2006 and in 2011. Now, in order -- the way it works is, the -- there is an application that is made by the FBI under the statute to the FISA court. We call it the FISC. They ask for and receive permission under the FISC under this to get records that are relevant to a national security investigation. And they must demonstrate to the FISC that it will be operated under the guidelines that are set forth by the attorney general under executive order 12333. This is what covers intelligence gathering in the federal government.

It is limited to tangible objects. Now, what does that mean? These are like records, like the metadata, the phone records I've been describing. But it is quite explicitly limited to things that you could get with a grand jury subpoena, those kinds of records. Now, it's important to know prosecutors issue grand jury subpoenas all the time and do not need any involvement of a court or anybody else,

really, to do so.

Under this program, we need to get permission from the court to issue this ahead of time. So there is court involvement with the issuance of these orders, which is different from a grand jury subpoena. But the type of records, just documents, business records, things like that, are limited to those same types of records that we could get through a grand jury subpoena.

Now, the orders that we get last 90 days. So we have to re-up and renew these orders every 90 days in order to do this. Now, there are strict controls over what we can do under the order. And, again, that's the bigger, thicker order that hasn't been published. There's restrictions on who can access it in this order. It is stored in repositories at NSA that can only be accessed by a limited number of people. And the people who are allowed to access it have to have special and rigorous training about the standards under which that they can access it.

In order to access it, there needs to be a finding that there is responsible suspicion that you can articulate, that you can put into words, that the person whose phone records you want to query is involved with some sort of terrorist organizations. And they are defined. It's not everyone. They are limited in the statute. So there has to be independent evidence, aside from these phone records, that the person you're targeting is involved with a terrorist organization.

COLE: If that person is a United States person, a citizen, or a lawful permanent resident, you have to have something more than just their own speeches, their own readings, their own First Amendment-type activity. You have to have additional evidence beyond that that indicates that there is reasonable, articulable suspicion that these people are associated with specific terrorist organizations.

Now, one of the things to keep in mind is under the law, the Fourth Amendment does not apply to these records. There was a case quite a number of years ago by the Supreme Court that indicated that toll records, phone records like this, that don't include any content, are not covered by the Fourth Amendment because people don't have a reasonable expectation of privacy in who they called and when they called. That's something you show to the phone company. That's something you show to many, many people within the phone company on a regular basis.

Once those records are accessed under this process and reasonable articulable suspicion is found, that's found by specially trained people. It is reviewed by their supervisors. It is documented in writing ahead of time so that somebody can take a look at it. Any of the accessing that is done is done in an auditable fashion. There is a trail of it. So both the decision and the facts that support the accessing and the query is documented. The amount that was done, what was done -- all of that is documented and reviewed and audited on a fairly regular basis.

There are also minimization procedures that are put into place so

that any of the information that is acquired has to be minimized. It has to be limited and its use is strictly limited. And all that is set out in the terms of the court order. And if any U.S. persons are involved, there are particular restrictions on how any information concerning a U.S. person can be used in this.

Now, there is extensive oversight and compliance that is done with these records and with this process. Every now and then, there may be a mistake -- a wrong phone number is hid or a person who shouldn't have been targeted gets targeted because there is a mistake in the phone record, something like that.

Each of those compliance incidents, if and when they occur, have to be reported to the FISA court immediately. And let me tell you, the FISA court pushes back on this. They want to find out why did this happen, what were the procedures and the mechanisms that allowed it to happen, and what have you done to fix it. So whenever we have a compliance incident, we report it to the court immediately and we report it to Congress. We report it to the Intelligence Committees of both houses and the Judiciary Committees of both houses.

We also provide the Intelligence and Judiciary Committees with any significant interpretations that the court makes of the 215 statute. If they make a ruling that is significant or issue an order that is significant in its interpretation, we provide those, as well as the applications we made for those orders, to the Intelligence Committee and to the Judiciary Committee.

And every 30 days, we are filing with the FISC, with the court, a report that describes how we implement this program. It includes a discussion of how we're applying the reasonable, articulable suspicion standard. It talks about the number of approved queries that we made against this database, the number of instances that the query results and contain a U.S. person information that was shared outside of NSA. And all of this goes to the court.

At least once every 90 days and sometimes more frequently, the Department of Justice, the Office of the Director of National Intelligence, and the NSA meet to assess NSA's compliance with all of these requirements that are contained in the court order. Separately, the Department of Justice meets with the inspector general for the National Security Agency and assesses NSA's compliance on a regular basis.

Finally, there is by statute reporting of certain information that goes to Congress in semiannual reports that we make on top of the periodic reports we make if there's a compliance incident. And those include information about the data that was required and how we are performing under this statute.

So once again keeping in mind, all of this is done with three branches of government involved: oversight and initiation by the executive branch with review by multiple agencies; statutes that are passed by Congress, oversight by Congress; and then oversight by the court.

Now, the 702 statute under the FISA Amendments Act is different.

Under this, we do get content, but there's a big difference. You are only allowed under 702 to target for this purpose non-U.S. persons who are located outside of the United States. So if you have a U.S. permanent resident who's in Madrid, Spain, we can't target them under 702. Or if you have a non-U.S. person who's in Cleveland, Ohio, we cannot target them under 702. In order to target a person, they have to be neither a citizen nor a permanent U.S. resident, and they need to be outside of the United States while we're targeting them.

Now, there's prohibitions in this statute. For example, you can't reverse-target somebody. This is where you target somebody who's out of the United States, but really your goal is to capture conversations with somebody who is inside the United States. So you're trying to do indirectly what you couldn't do directly. That is explicitly prohibited by this statute. And if there is ever any indication that it's being done, because again, we report the use that we make of this statute to the court and to the Congress, that is seen.

You also have to have a valid foreign intelligence purpose in order to do any of the targeting on this. So you have to make sure, as it was described, that it's being done for defined categories of weapons of mass destruction, foreign intelligence, things of that nature. These are all done pursuant to an application that is made by the attorney general and the director of national intelligence to the FISC. The FISC gives a certificate that allows this targeting to be done for a year period. It then has to be renewed at the end of that year in order for it to be re-upped.

Now, there's also there is a requirement that, again, there is reporting. You cannot under the terms of this statute have and collect any information on conversations that are wholly within the United States. So you're targeting someone outside the United States. If they make a call to inside the United States, that can be collected, but it's only because the target of that call outside the United States initiated that call and went there. If the calls are wholly within the United States, we cannot collect them.

If you're targeting a person who is outside of the United States and you find that they come into the United States, we have to stop the targeting right away. And if there's any lag and we find out that we collected information because we weren't aware that they were in the United States, we have to take that information, purge it from the systems, and not use it.

Now, there's a great deal of minimization procedures that are involved here, particularly concerning any of the acquisition of information that deals or comes from U.S. persons. As I said, only targeting people outside the United States who are not U.S. persons. But if we do acquire any information that relates to a U.S. person, under limited criteria only can we keep it.

If it has to do with foreign intelligence in that conversation or understanding foreign intelligence, or evidence of a crime or a threat of serious bodily injury, we can respond to that. Other than that, we have to get rid of it. We have to purge it, and we can't use it. If we inadvertently acquire any of it without meaning to, again, once that's discovered, we have to get rid of it. We have to purge it.

The targeting decisions that are done are, again, documented ahead of time, reviewed by a supervisor before they're ever allowed to take place in the beginning. The Department of Justice and the Office of the Director of National Intelligence conduct on-site reviews of each targeting that is done. They look at them to determine and go through the audit to determine that they were done properly. This is done at least every 60 days and many times done more frequently than that.

In addition, if there's any compliance issue, it is immediately reported to the FISC. The FISC, again, pushes back: How did this happen? What are the procedures? What are the mechanisms you're using to fix this? What have you done to remedy it? If you acquired information you should (sic) have, have you gotten rid of it as you're required? And in addition, we're providing Congress with all of that information if we have compliance problems.
We also report quarterly to the FISC concerning the compliance issues that have arisen during that quarter, on top of the immediate reports and what we've done to fix it and remedy the ones that we reported.

COLE: We also to Congress under this program, the Department of Justice and the Office of the Director of National Intelligence provide a semiannual report to the FISC and to Congress assessing all of our compliance with the targeting and minimization procedures that are contained in the court order. We also provide a semi-annual report to the FISC and Congress concerning the implementation of the program, what we've done and what we've found. And we also provide to Congress, documents that contain again, how we're dealing with the minimization procedures, any significant legal interpretations that the FISC makes concerning these statutes, as well as the orders and the applications that would relate to that.

And on top of all of this, annually the inspector general for NSA does an assessment, which he provides to Congress that reports on compliance, the number of disseminations under this program that relate to U.S. persons, the number of targets that were reasonably believed at the time to be outside the United States who were later determined to be in the United States, and when that was done. So in short, there is, from before, during and after the involvement of all three branches of the United States government, on a robust and fairly intimate way. I'd like to make one other observation, if I may, on this. We have tried to do this in as thorough, as protective, and as transparent a way as we possibly can, considering it is the gathering of intelligence information.

Countries and allies of ours all over the world collect intelligence. We all know this. And there have recently been studies about how transparent our system is in the United States, compared to many of our partners, many in the E.U. Countries like France, the U.K., Germany, who we work with regularly. And a report that was just recently issued in May of this year found that the FISA Amendments Act, the statute that we're talking about here, and I will quote, "Imposes at least at much, if not more, due process and oversight on foreign intelligence surveillance than other countries." And this

includes E.U. countries. And it says under this, the U.S. is more transparent about its procedures, requires more due process protections in its investigations that involve national security, terrorism and foreign intelligence.

The balance is always one we seek to strive to -- to achieve. But I think as I've laid out to you, we have done everything we can to achieve it. And I think part of the proof of what we've done is this report that came out just last month, indicating our system is as good, and frankly better, than all of our allies and liaison partners. Thank you Mr. Chairman.

ALEXANDER: Mr. Chairman, I will now switch to the value of the program, and talk about some statistics that we're putting together. As we stated, these programs are immensely valuable for protecting our nation, and security the security of our allies. In recent years, the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world. FAA 702 contributed in over 90 percent of these cases. At least 10 of these events included homeland-based threats. In the vast majority, business records, FISA reporting contributed as well. I would also point out that it is a great partnership with the Department of Homeland Security in those with a domestic nexus.

But the real lead for domestic events is the Federal Bureau of Investigation. It has been our honor and privilege to work with Director Mueller, and Deputy Directory Joyce who -- I'll turn it now over to Sean?

JOYCE: Thank you General. Thank you chairman and ranking member, and members of the committee for the opportunity to be here today. NSA and the FBI have a unique relationship, and one that has been invaluable since 9/11. And I just want to highlight a couple of the instances. In the fall of 2009, NSA using 702 authority intercepted an e-mail from a terrorist located in Pakistan. That individual was talking with an individual located inside the United States, talking about perfecting a recipe for explosives. Through legal process, that individual was identified as Najibullah Zazi. He was located in Denver, Colorado.

The FBI followed him to New York City. Later we executed search warrants with the New York Joint Terrorism Task Force and NYPD and found bomb-making components in backpacks. Zazi later confessed to a plot to bomb the New York subway system with backpacks. Also working with FISA business records, the NSA was able to provide a previously unknown number of one of the co-conspirators -- co-conspirators, Adis Medunjanin. This was the first core Al Qaida plot since 9/11 directed from Pakistan. Another example, NSA utilizing 702 authority was monitoring a known extremist in Yemen. This individual was in contact with an individual in the United States named Khalid Ouazzani. Ouazzani and other individuals that we identified through a FISA that the FBI applied for through the FISC were able to detect a nascent plotting to bomb the New York Stock Exchange.

Ouazzani had been providing information and support to this plot. The FBI disrupted and arrested these individuals. Also David Headley, a U.S. citizen living in Chicago. The FBI received intelligence

regarding his possible involvement in the 2008 Mumbai attacks responsible for the killing of over 160 people. Also, NSA through 702 coverage of an Al Qaida affiliated terrorist found that Headley was working on a plot to bomb a Danish newspaper office that had published the cartoon depictions of the Prophet Mohammed. In fact, Headley later confessed to personally conducting surveillance of the Danish newspaper office. He, and his co-conspirators were convicted of this plot.

Lastly, the FBI had opened an investigation shortly after 9/11. We did not have enough information, nor did we find links to terrorism and then we shortly thereafter closed the investigation. However, the NSA using the business record FISA tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process, and were able to disrupt this terrorist activity. Thank you. Back to you, General?

ALEXANDER: So that's four cases total that we've put out publicly. What we're in the process of doing with the inter-agency is looking at over 50 cases that were classified, and will remain classified, that will be provided to both of the Intel Committees of the Senate and the House, to all of you. Those 50 cases right now have been looked at by the FBI, CIA and other partners within the community, and the National Counterterrorism Center is validating all of the points so that you know that what we've put in there is exactly right. I believe the numbers from those cases is something that we can publicly reveal, and all publicly talk about.

What we are concerned, as the chairman said, is to going into more detail on how we stopped some of these cases, as we are concerned it will give our adversaries a way to work around those, and attack us, or our allies. And that would be unacceptable. I have concerns that the intentional and irresponsible release of classified information about these programs will have a long, and irreversible impact on our nation's security, and that of our allies. This is significant. I want to emphasize that the Foreign Intelligence is the best -- the Foreign Intelligence Program that we're talking about, is the best counterterrorism tools that we have to go after these guys.

We can't lose those capabilities. One of the issues that has repeatedly come up, well how do you then protect civil liberties and privacy? Where is the oversight? What are you doing on that? We have the deputy director of the National Security Agency, Chris Inglis, will now talk about that and give you some specifics about what we do, and how we do it with these programs.

INGLIS: Thank you, General Alexander.

Chairman, Ranking Member, members of the committee, I'm pleased to be able to briefly describe the two programs as used by the National Security Agency with a specific focus on the internal controls and the oversight provided. Now first to remind these two complimentary, but distinct programs are focused on foreign intelligence. That's NSA's charge. The first program executed under Section 215 of the Patriot Act authorizes he collection of telephone metadata only. As you've heard before, the metadata is only the

telephone numbers, and contact, the time and date of the call, and the duration of that call.

INGLIS: This authority does not, therefore, allow the government to listen in on anyone's telephone calls, even that of a terrorist. The information acquired under the court order from the telecommunications providers does not contain the content of any communications, what you are saying during the course of the conversation, the identities of the people who are talking, or any cell phone locational information. As you also know this program was specifically developed to allow the U.S. government to detect communications between terrorists operating outside the U.S., who are themselves communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11.

The controls on the use of this data at NSA are specific, rigorous, and designed to ensure focus on counter-terrorism. To that end, the metadata acquired and stored under this program may be queried only when there is a reasonable suspicion based on specific and documented facts that an identifier, like a telephone number, is associated with specific foreign terrorist organizations.

This determination is formally referred to as the "reasonable articulable suspicion standard." During all 2012, the 12 months of 2012, we at NSA approved fewer than 300 unique numbers, which were then used to initiate a query of this data set.

The second program, authorized under Section 702 of the Foreign Intelligence Surveillance Act, authorizes targeting only for communications of foreigners who are themselves not within the United States for foreign intelligence purposes, with the compelled assistance of an electronic communications service provider.

As I noted earlier, NSA being a foreign intelligence agency, foreign intelligence for us is information related to the capabilities, intentions, or activities of foreign governments, foreign organizations, foreign persons, or international terrorists. Let me be very clear. Section 702 cannot be and is not used to intentionally target any U.S. citizen or any U.S. person, any person known to be in the United States, a person outside the United States if the purpose is to acquire information from a person inside the United States. We may not do any of those things using this authority.

The program is also key in our counter-terrorism efforts, as you've heard. More than 90 percent of the information used to support the 50 disruptions mentioned earlier was gained from this particular authority. Again, if you want to target the content of a U.S. person anywhere in the world, you cannot use this authority. You must get a specific court warrant.

I'd like to now describe in further details some of the rigorous oversight for each of these programs. First, for the Section 215 program, also referred to as business records FISA, controls and (ph) determine how we manage and use the data are explicitly defined and formally approved by the Foreign Intelligence Surveillance Court.

First, the metadata segregated from other data sets held by NSA and all queries against the data base are documented and audited. As defined in the orders of the court, only 20 analysts at NSA and their two managers, for a total of 22 people, are authorized to approve numbers that may be used to query this database. All of those individuals must be trained in the specific procedures and standards that pertain to the determination of what is meant by reasonable, articulable suspicion.

Every 30 days, NSA reports to the court the number of queries and disseminations made during that period. Every 90 days, the Department of Justice samples all queries made across the period and explicitly reviews the basis for every U.S. person, or every U.S. identity query made. Again, we do not know the names of the individuals of the queries we might make.

In addition, only seven senior officials at NSA may authorize the dissemination of any information we believe that might be attributable to a U.S. person. Again, we would not know the name. It would only be the telephone number. And that dissemination in this program would only be made to the Federal Bureau of Investigation at determining that the information is related to and necessary to understand a counter-terrorism initiative.

The Foreign Intelligence Surveillance court reviews the program every 90 days. The data that we hold must be destroyed within five years of its acquisition. NSA and the Department of Justice briefed oversight committees on the employment of the program. We provide written notification of all significant developments within the program. The Department of Justice provides oversight committees with all significant foreign intelligence surveillance courts' opinions regarding the program.

Turning my attention to the 702 program, the Foreign Intelligence Surveillance Court annually reviews certification, which are required by law, that are jointly submitted by the attorney general and the director of national intelligence. These certifications define the categories of foreign actors that may be appropriately targeted and, by law, must include specific targeting and minimization procedures that the attorney general and the court both agree are consistent with the law and the Fourth Amendment of the Constitution. These procedures require that a communication of or concerning a U.S. person must be promptly destroyed after it's identified, either as clearly not relevant to the authorized purpose, or as not containing evidence of a crime.

The statute further requires a number of reports to be provided to both the court and the oversight committees. A semi-annual assessment by the Department of Justice and the Office of the Director of National Intelligence, regard in (ph) compliance with the targeting and minimization procedures an annual I.G. assessment that reports compliance with procedural requirements laid out within the order -- the number of disseminations that may refer to U.S. persons, the number of targets later found to be in the United States, and whether the communications of such targets were ever reviewed.

An annual director of NSA report is also required to describe the compliance efforts taken by NSA and address the number of U.S. person identities disseminated in NSA reporting. Finally, Foreign Intelligence Surveillance Court procedures require NSA to inform the court of any novel issues of law or technology relevant to an authorized activity and any non-compliance to include the Executive Branch's plan for remedying that same event. In addition to the procedures I've just described, the Department of Justice conducts on-site reviews at NSA to sample NSA's 702 targeting and tasking decisions every 60 days.

And, finally, I would conclude with my section to say that in July of 2012, the Senate Select Committee on Intelligence, in a report reviewing the progress over the four years of the law's life at that point in time, said that across the four-year history of the program, the committee had not identified a single willful effort by the Executive Branch to violate the law.

ALEXANDER: So to wrap up, Chairman, first I'd like to just hit on -- when we say seven officials, that's seven positions that -- at NSA can disseminate U.S. persons data. Today, there are 10 people in those positions. One of those is our -- SIGINT operations officer. Every one of those have to be -- credentialed. Chris and I are two of those officials.

I do want to hit a couple of key points. First, with our industry partners, under the 702 program, the U.S. government does not unilaterally obtain information from the servers of U.S. companies. Rather, the U.S. companies are compelled to provide these records by U.S. law, using methods that are in strict compliance with that law.

Further, as the deputy attorney general noted, virtually all countries have lawful intercept programs under which they compel communication providers to share data about individuals they believe represent a threat to their societies. Communication providers are required to comply with those programs in the countries in which they operate. The United States is not unique in this capability.

The U.S., however, operates its program under the strict oversight and compliance regime that was noted above with careful oversights by the courts, Congress, and the administration. In practice, U.S. companies have put energy and focus and commitment into consistently protecting the privacy of their customers around the world, while meeting their obligations under the laws of U.S. and other countries in which they operate. And I believe they take those seriously.

Our third and final point, as Americans, we value our privacy and our liberty -- our civil liberties. Americans -- as Americans, we also value our security and our safety. In the 12 years since the attacks on September 11th, we have lived in relative safety and security as a nation. That security is a direct result of the intelligence community's quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11.

In those 12 years, we have thought long and hard about oversight

and compliance and how we minimize the impact on our fellow citizens' privacy. We have created and implemented and continue to monitor -- monitor a comprehensive mission compliance program inside NSA. This program, which was developed based on industry best practices and compliance works to keep operations and technology aligned with NSA's externally approved procedures.

Outside of NSA, the officer of the -- the Office of the Director of National Intelligence, Department of Justice, and the Foreign Intelligence Surveillance Court provide robust oversight as well as this committee. I do believe we have that balance right.

In summary, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community's efforts to connect the dot. Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes and oversight mechanisms. Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people.

As you noted, Chairman, the people of NSA take these responsibilities to heart. They protect our nation and our allies as part of a bigger team. And they protect our civil liberties and privacy. It has been an honor and privilege to lead these great Americans. I think Bob Litt has a couple of comments to make, and then we'll turn it back to you, Chairman.

LITT: Yes, Mr. Chairman, Mr. Ranking Member, members of the committee, I just want to speak very briefly and address a couple of additional misconceptions that the public has been fed about some of these programs.

The first is that collection under Section 702 of the FISA Amendments Act is somehow a loosening of traditional standards because it doesn't require individualized warrants. And, in fact, exactly the opposite is the case. The kind of collection that is done under Section 702, which is collecting foreign intelligence information for foreigners outside of the United States historically was done by the executive branch under its own authority without any kind of supervision whatsoever.

And as a result of the FISA Amendments Act, this has now been brought under a judicial process with the kind of restrictions and limitations that have been described by the other witnesses here. So, in fact, this is a tightening of standards from what they were before.

The second misconception is that the FISA court is a rubber stamp for the executive branch. And people point to the fact that the FISA court ultimately approves almost every application that the government submits to it.

But this does not recognize the actual process that we go through with the FISA court. The FISA court is judges, federal district judges appointed from around the country who take this on in addition to their other burdens. They're all widely respected and experienced judges. And they have a full-time professional staff that works only

on FISA matters.

When we prepare an application for -- for a FISA, whether it's under one of these programs or a traditional FISA, we first submit to the court what's called a "read copy," which the court staff will review and comment on.

And if -- and they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the government and the FISA court to take care of those concerns so that at the end of the day, we're confident that we're presenting something that the FISA court will approve. That is hardly a rubber stamp. It's rather extensive and serious judicial oversight of this process.

The third point, the third misconception that I want to make is that the process we have here is one that simply relies on trust for individual analysts or individual people at NSA to obey the rules.

And I just -- I -- I won't go into detail as to the oversight, because I think it's been adequately described by the others. But the point is, there is a multilayered level of oversight, first within NSA, then involving my agency, the Office of the Director of National Intelligence and the Department of Justice and ultimately involving the FISA court and the Congress to ensure that these rules are complied with.

And the last point that I'd -- the last misconception I want to address is that this information shouldn't have been classified and it was classified only to -- to conceal it from the American people and that the leaks of this information are not damaging.

And, Mr. Chairman and Mr. Ranking Member, you both made this point. These are, as General Alexander said, extremely important collection programs to protect us not only from terrorists, but from other threats to our national security, a wide variety.

And they have produced a huge amount of valuable intelligence over the years. We are now faced with a situation that because this information has been made public, we run the risk of losing these collection capabilities. We're not gonna know for many months whether these leaks in fact have caused us to lose these capabilities. But if -- if they -- if they do have that effect, there is no doubt that they will cause our national security to be affected.

Thank you, Mr. Chairman.

ROGERS: Thank you all, very much. I appreciate that. I just have a couple of quick questions. I know members have lots of questions here and I want to get to them.

Mr. Inglis, just for the record, you -- can you describe quickly your civilian role as the deputy? You serve as that role in a civilian capacity. Is that correct?

INGLIS: Yes, sir. Across the history of NSA, there has always been a senior serving military officer, that's the director of the

National Security Agency, and at the same time a senior serving civilian authority, and that would be the deputy director, and that's my role.

ROGERS: All right, and -- but you have also had military service. Is that correct?

INGLIS: Sir, I did. I served for a period of 13 years on active duty in the United States Air Force, and then transitioned to the National Security Agency.

ROGERS: So you rose to the rank of -- of?

INGLIS: I was brigadier general in the Air National Guard. As in all things, it's complicated.

(CROSSTALK)
ROGERS: Yeah. But I just wanted to get on the record that you do have -- you have military service as well as your civilian service.

(CROSSTALK)

INGLIS: I do, sir. As I transitioned from the active Air Force to the National Security Agency, I retained my affiliation with the reserve components and was pleased and proud to be able to serve in the Air National Guard for another 20 years.

ROGERS: Great. Well, thank you for that service.

You mentioned in "queries of less than 300," what does -- what does that mean?

INGLIS: In each of those cases, sir, there was a determination made an analyst at NSA that there was a reasonable, describable, articulable suspicion that an number of interest, a telephone number of interest, might be associated with a connected plot of a specific terrorist plot overseas, and therefore a desire to see whether that plot had a connection into the United States.

The process they go through then is as described, one where they make a -- a...

(CROSSTALK)

ROGERS: Well, describe the inquiry -- it's not put -- you don't put in a name?

INGLIS: We do not, sir.

ROGERS: So you put in...

(CROSSTALK)

INGLIS: The only thing we get from the providers are numbers. The only thing we could possibly then bounce against that data set are numbers, themselves.

ROGERS: Right. So there are no names and no addresses affiliated with these phone numbers.

INGLIS: No, there are not, sir.

ROGERS: OK. Just phone numbers.

INGLIS: That's right, sir.

ROGERS: OK. Go ahead.

INGLIS: So an analyst would then try to determine whether there was a describable, it must be written, documentation that would say that there is a suspicion that this is attributed to a foreign terrorist plot and there might be a U.S. nexus.
After having made that determination, they would make a further check to determine whether it is possible to discern that this might be associated with a U.S. person. The way you would infer that is you might look at the area code and say that area code could likely be in the United States. We all know that within this area, that if you see an area code that begins with 301, that would be Maryland. That would be your only insight into whether or not this might be attributable to a U.S. person.

If that were to be the case, then the case for a reasonable, articulable suspicious must get a further review to ensure that this is not a situation where somebody is merely expressing their First Amendment rights.

If that's all that was, if they were merely expressing their First Amendment rights, however objectionable any person might find that, that is not a basis to query the database.

If it gets through those checks, then at that point, it must be approved by one of those 20 plus two individuals -- 20 analysts, specially-trained analysts, or their two managers -- such that it might then be applied as a query against the data set. Again, the query itself would just be a number, and the query against the data set would then determine whether that number exists in the database. That's how that query is formed. And, again...

(CROSSTALK)

ROGERS: So the response is not a name; it's an address. It's a phone number.

INGLIS: It cannot be. If it were to be a name or if it were to be an address, there would be no possibility that the database would return any meaningful results, since none of that information is in the database.

ROGERS: Just a phone number pops back up.

INGLIS: Just a phone number. What comes back if you query the database are phone numbers that were in contact, if there are any, with that number. And, again, the other information in that database would indicate when that call occurred and what the duration of that

call were -- were to be.

ROGERS: Again, I just want to make very clear, there are no names and no addresses in that database.

INGLIS: There are not, sir.

ROGERS: OK. And why only less than 300 queries of phone numbers into that database?

INGLIS: Sir, only less than 300 numbers were actually approved for query against that database. Those might have been applied multiple times, and therefore, there might be a number greater than that of actual queries against the database.
But the reason there are so few selectors approved is that the court has determined that there is a very narrow purpose for this -- this use. It can't be to prosecute a greater understanding of a simply domestic plot. It cannot be used to do anything other than terrorism. And so, therefore, there must be very well-defined describable written determinations that this is -- is a suspicion of a connection between a foreign plot and a domestic nexus. If it doesn't meet those standards...

(CROSSTALK)

ROGERS: Are those queries reported to the court?

INGLIS: Those queries are all reported to the Department of Justice, reviewed by the Department of Justice. The number of those queries are reported to the court. And any time that there is a dissemination associated with a U.S. person...

(CROSSTALK)

ROGERS: Is there a court-approved process in order to make that query into that information of only phone numbers?

INGLIS: Yes, sir. The court explicitly approves the process by which those determinations were made, and the Department of Justice provides a rich oversight auditing of that capability.

ROGERS: Great. Thank you.

General Alexander, is the NSA on private company's servers as defined under these two programs?

ALEXANDER: We are not.

ROGERS: Is -- is the NSA have the ability to listen to Americans' phone calls or read their e-mails under these two programs?

ALEXANDER: No, we do not have that authority.

ROGERS: Does the technology exist at the NSA to flip a switch by some analyst to listen to Americans' phone calls or read their e-mails?

ALEXANDER: No.

ROGERS: So the technology does not exist for any individual or group of individuals at the NSA to flip a switch to listen to Americans' phone calls or read their e-mails?

ALEXANDER: That is correct.

ROGERS: When -- Mr. Joyce, if you could help us understand that, if you get a piece of a number, there's been some public discussion that, gosh, there's just not a lot of value in what you might get from a program like this that has this many levels of oversight. Can you talk about how that might work into an investigation to help you prevent a terrorist attack in the United States?

JOYCE: Investigating terrorism is not an exact science. It's like a mosaic. And we try to take these disparate pieces and bring them together to form a picture. There are many different pieces of intelligence. We have assets. We have physical surveillance. We have electronic surveillance through a legal process; phone records through additional legal process; financial records.

Also, these programs that we're talking about here today, they're all valuable pieces to bring that mosaic together and figure out how these individuals are plotting to attack the United States here or whether it's U.S. interests overseas.

So, every dot, as General Alexander mentioned, we hear the cliche frequently after 9/11 about connecting the dots. I can tell you as a team, and with the committee and with the American public, we come together to put all those dots together to form that picture to allow us to disrupt these activities.

ROGERS: Thank you.

Given the large number of questions by members, I'm going to move along.

Mr. Ruppersberger, for a brief...

RUPPERSBERGER: Firstly, I want to thank all the witnesses for your presentation, especially Mr. Cole -- a very good presentation. I think you explained the law in a very succinct way.

You know, it's unfortunate sometimes when we have incidents like this that a lot of negative or false information gets out. I think, though, that those of us who work in this field, in the intelligence field every day, know what the facts are and we're trying to now present those facts through this panel. That's important.

But I would say that I weren't in this field and if I were to listen to the media accounts of what occurred in the beginning, I would be concerned, too. So, this is very important that we get the message out to the American public that what we do is legal and we're doing it to protect our national security from attacks from terrorists.

Now, there are -- one area that, Mr. Litt, you -- you addressed this -- but I think it's important to just reemphasize the FISA court. You know, again, it's unfortunate, when people disagree with you, they attack you. They say things that aren't true. We know that these are federal judges in the FISA court. They have integrity, and that they will not approve anything that they feel is wrong. We have 90-day periods where the court looks at this issue.

I want to ask you, though, General Alexander, do you feel in any way that the FISA court is a rubber-stamp based on the process? Our forefathers created a great system of government, and that's checks and balances. And that's what we are. That's what we do in this country to follow our Constitution. It's unfortunate that these federal judges are being attacked.

ALEXANDER: I do not. I believe, as you have stated, the federal judges on that court are superb. Our nation would be proud of what they do and the way they go back and forth to make sure we do this exactly right.

And every time we make a mistake, how they work with us to make sure it is done correctly to protect our civil liberties and privacy and go through the court process. They have been extremely professional. There is, from my perspective, no rubber-stamp.

It's kind of interesting. It's like saying you just ran a 26-mile marathon; somebody said, "Well, that was just a jog." Every time we work with the court, the details and the specifics of that that go from us up through the FBI, through the Department of Justice and through the court on each one of those orders that we go to the court. There is tremendous oversight, compliance and work. And I think the court has done a superb job.

More importantly, if I could, what we worked hard to do is to bring all of these -- all these under court supervision for just this reason. I mean, we've done the right thing, I think, for our country here.

Thank you.

RUPPERSBERGER: Thank you for that answer.

The second area I want to get into, General Alexander, the public are saying, "Well, how did this happen?" We have -- we have rules. We have regulations. We have individuals that work in intelligence go through being -- persistently being classified. And yet here we have a technical person who had lost some jobs; had a background that wouldn't always would be considered the best.

We have to learn from mistakes how they've occurred. What system are you or the director of national intelligence of the administration putting into effect now to make sure what happened in this situation, that if another person were to -- to turn against his or her country, that we would have an alarm system that would not put us in this position right now?

ALEXANDER: So, this is a very difficult question, especially when that person is a system administrator and they get great access...

RUPPERSBERGER: Why don't you say what a system administrator is?

ALEXANDER: Well, a system administrator is one that actually helps operate, run, set the conditions, the auditing and stuff on a system or a portion of the network. When one of those persons misuses their authorities, this is a huge problem.

So working with the director of national intelligence, what we are doing is working to come up with a two-person rule and oversight for those, and ensure that we have a way of blocking people from taking information out of our system. This is work in progress. We're working with the FBI on the investigation. We don't have all the facts yet. We've got to get those. And as we're getting those facts, we are working through our system. Director Clapper has asked us to do that and providing that feedback back to the rest of the community.

RUPPERSBERGER: OK. Thank you.

I yield back.

ROGERS: (OFF-MIKE)

THORNBERRY: Thank you, Mr. Chairman.

And thank you all for being here, and for making some additional information available to the public. I know it's frustrating for you, as it is for us, to have these targeted narrow leaks and not be able to talk about the bigger picture.

General Alexander, you mentioned that you're going to send us tomorrow 50 cases that have been stopped because of these programs, basically. Four have been made public to this point. And I think there are two new ones that you are talking about today. But I would invite you to explain to us both of those two new cases -- Mowlin (ph) and the Operation WiFi case. And one of them starts with a 215; one of them starts with a 702.

And so I think it's important for you to provide the information about how these programs stopped those terrorist attacks.

ALEXANDER: OK. I'm going to defer this, because the actual guys who actually do all the work and (inaudible) is the FBI, and get it exactly right. I'm going to have Sean do that. Go ahead, Sean.

JOYCE: So, Congressman, as I mentioned previously, NSA on the Op WiFi, which is Khalid Ouazzani out of Kansas City. That was the example that I referred to earlier. NSA, utilizing 702 authority, identified an extremist located in Yemen. This extremist located in Yemen was talking with an individual located inside the United States in Kansas City, Missouri. That individual was identified as Khalid Ouazzani.

The FBI immediately served legal process to fully identify Ouazzani. We went up on electronic surveillance and identified his co-conspirators. And this was the plot that was in the very initial stages of plotting to bomb the New York Stock Exchange. We were able to disrupt the plot. We were able to lure some individuals to the United States. And we were able to effect their arrest. And they were convicted for this terrorist activity.

THORNBERRY: OK. Just so I -- on that plot, it was under the 702, which is targeted against foreigners, that some communication from this person in Yemen back to the United States was picked up. And then they turned it over to you at the FBI to serve legal process on this person in the United States.

JOYCE: That is absolutely correct. And if you recall, under 702, it has to be a non-U.S. person outside the United States, and then also one of the criteria is linked to terrorism.

THORNBERRY: OK. Would you say that this -- their intention to blow up the New York Stock Exchange was a serious plot? Or is this something that they kind of dreamed about, you know, talking among their buddies?

JOYCE: I think the jury considered it serious, since they were all convicted.

THORNBERRY: OK. And -- and what about the other plot? October, 2007, that started I think with a 215?

JOYCE: I refer to that plot. It was an investigation after 9/11 that the FBI conducted. We conducted that investigation and did not find any connection to terrorist activity. Several years later, under the 215 business record provision, the NSA provided us a telephone number only, in San Diego, that had indirect contact with an extremist outside the United States.

We served legal process to identify who was the subscriber to this telephone number. We identified that individual. We were able to, under further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA court, we were able to identify co-conspirators and we were able to disrupt this terrorist activity.

THORNBERRY: I'm sorry. Repeat for me again what they were plotting to do.

JOYCE: He as actually -- he was providing financial support to an overseas terrorist group that was a designated terrorist group by the United States.

THORNBERRY: But there was some connection to suicide bombings that they were talking about, correct?

JOYCE: Not in the example that I'm citing right here.

THORNBERRY: Oh, I'm sorry, the group in Somalia to which he was

financing, that's what they -- that's what they do do in Somalia, correct?

JOYCE: That is correct, and as you know, as part of our classified hearings regarding the American presence in -- in that area of the world.

THORNBERRY: OK. OK, thank you.

Chairman (OFF-MIKE)

ALEXANDER: If I could, Congressman, just -- just hit a couple key points. It's over 50 cases. And the reason I'm not giving a specific number is we want the rest of the community to actually beef those up and make sure that (inaudible) we have there is exactly right. I'd give you the number 50X. But if somebody says, "Well, not this one." Actually, what we're finding out is there are more. They said, "You missed these three or four." So those are being added to the packet.

On the top of that packet we'll have a summary of all of these, the listing of those. I believe those numbers are things that we can make public, that you can use, that we can use. And we'll try to give you the numbers that apply to Europe, as well, as well as those that had a nexus in the United States.

The issue on terms of releasing more on the specific overseas cases is (inaudible) our -- it's our concern that in some of those -- now, going into further details of exactly what we did and how we did it may prevent us from disrupting a future plot.

So that's something that work in progress. Our intent is to get that to the committee tomorrow for both -- both Intel Committees for the Senate and House.

THORNBERRY: Great. Thank you.

ROGERS: Mr. Thompson?

THOMPSON: Thank you, Mr. Chairman.

Thank you all very much for being here and for your testimony and for your service to our country.

Mr. Litt, before going to a hearing, does or has the FISA court ever rejected a case that's been brought before it?

LITT: I believe the answer to that is yes, but I would defer that to the deputy attorney general.

COLE: It has happened. It's not often, but it does happen.

THOMPSON: Thank you.

Mr. Cole, what kinds of records comprise the data collected under the business records provision?

COLE: There's a couple of different kinds. The shorthand -- and it's required under the statute -- is the kinds of records you could get with a grand jury subpoena. These are business records that already exist. It could be a contract. It could be something like that.

In this instance that we're talking about for this program, these are telephone records. And it's just like your telephone bill. It'll show a number called, the date the number was called, how long the call occurred; a number that called back to you. That's all it is, not even identifying who the people are that's involved.

THOMPSON: Have you previously collected anything else under that authority?

COLE: Under the 215 authority?

THOMPSON: Correct.

COLE: I'm not sure beyond the 215 and the 702 that -- answering about what we have and haven't collected has been declassified to be talked about.

THOMPSON: OK.

It was said that there's been cases where there was data inadvertently or mistakenly collected and then subsequently destroyed. Is that...

COLE: That's correct.

THOMPSON: And -- and there actually has been data that has been inadvertently collected and it was destroyed, nothing else was done with it?

COLE: That's correct. The -- this is a very strict process that we go through in that regard. You can get a wrong digit on a phone number and you collect the wrong number, something like that. And when that's discovered, that's taken care of in that way.

THOMPSON: And who does the checking? Who -- who determines if something has been inadvertently collected and then decides that it's -- needs to be destroyed?

COLE: Well, I'll -- I'll refer over to NSA in the first instance, because they do a very robust and vigorous check internally themselves. But then as an after-the-fact, the Department of Justice and ODNI and the inspector general for NSA also do audits and make sure that we understand all the uses. And if there's any compliance problems that they're identified, that they're given to the court, they're given to the Congress, and they're fixed.

THOMPSON: I -- I don't think I need anything more than -- than that.

General Alexander, can you tell us what Snowden meant during this chat thing that he did when he said that NSA provides Congress with,

and I quote, "a special immunity to its surveillance"?

ALEXANDER: I have no idea.

THOMPSON: Anybody else?

ALEXANDER: I'm not sure I understand the context of the special immunity.

THOMPSON: I -- I don't either. That's why...

(CROSSTALK)

ALEXANDER: We treat you with special respect.

(LAUGHTER)

THOMPSON: He said with a "special immunity to its surveillance."

ALEXANDER: I -- I have no idea. I think it may be in terms of disseminating any information, let's say, not in this program but in any program that we have, if we have to disseminate U.S. persons data or a threat to a U.S. member of Congress, we're not allowed to say the name unless it's valuable to one of the investigations or (inaudible).

So we can't just put out names and stuff in our things (ph). So part of the minimization procedures protects the who.

Did you want to add to that?

INGLIS (?): No, I would simply have said that your status as U.S. persons gives you a special status, as we've described throughout this hearing.
THOMPSON: If you -- if that does surface and you do figure that out you'll get that information to us?

Also the president kind of suggested, I guess, in his television interview the other night that the New York subway bomber could not have been or would not have been caught without PRISM. Is that true?

JOYCE: Yes, that is accurate. Without the 702 tool we would not have identified Najibullah Zazi.

THOMPSON: Thank you. I have no further question.

I yield back the balance of my time.

ROGERS: Mr. Miller?

MILLER: Thank you, Mr. Chairman.

General Alexander, which agency actually presents the package to the FISA court for them to make their decision?

ALEXANDER: Well, it's actually -- business records, FISA, it's the FBI (inaudible).

Go ahead.

JOYCE: The FBI is part of the process. It then goes over to the Department of Justice. And they are the ones -- if the DAG wants to comment on that.

COLE: The formal aspect of the statute allows the director of the FBI to make an application to the court. The Justice Department handles that process. We make the -- put all the paperwork together. And it must be signed off on before it goes to the court by either the attorney general, myself, or if we have a confirmed assistant attorney general in charge of the National Security Division, that person is authorized. But it has to be one of the three of us to sign it before it goes.

MILLER: The court is a single judge?

COLE: The judges sit kind of in -- in rotation in the court presiding over it. These are all Article 3 judges. They have lifetime appointments. They have their districts that they deal with, and they are selected by the chief justice to sit on the FISA court for a period of time. And so they will rotate through and be the duty judges that are required for this.

MILLER: I guess the crux of my question is, would there be a way that if you did not get the answer that you wanted from a certain judge could you go to another FISA court judge and ask for another opinion?

COLE: I -- I think that would be very, very difficult to do, because the staff at the FISA court does a great deal of the prep work and they're gonna recognize when they've thrown something back that if you're coming back and you haven't made any changes to correct the deficiencies that caused them to throw it back, my guess is they'll throw it back again.

MILLER: And I think one of the things that a lot of people don't understand -- and it was alluded to by Mr. Litt; and I think, Mr. Cole, you have also discussed it -- and that's the read-ahead document that the court gets, the opportunity. A lot of focus has been made on the fact that as my colleague, Mr. Thompson said, court's a rubberstamp. But they do have an opportunity to review the documents prior to rendering a decision.

COLE: They do. And it's by no means as a rubber stamp. They push back a lot. And when they see something -- these are very thick applications that have a lot in them. And when they see anything that raises an issue, they will push back and say, "We need more information about this area. We need more information about that legal issue. We need more information about your facts in certain areas.'

This is by no means a rubberstamp. There is an enormous amount of work. And they make sure -- they're the ones to make sure that the privacy and the civil liberty interests of United States' citizens are honored. They're that bulwark in this process. So they -- they have to be satisfied.

MILLER: There's been some discussion this morning on the inadvertent violation of a court order where data has been collected and then destroyed. But has there ever been any disciplinary action taken on somebody who inadvertently violated an order?

COLE: Not that I'm aware of. And I think one of the statistics that Mr. Inglis had included in his comment was that in the history of this, there has never been found an intentional violation of any of the provisions of the court order, or any of the collection in that regard. So the -- the nature of the kinds of anomalies that existed were technical errors, were typographical errors, things of that nature as opposed to anything that was remotely intentional. So there would be in those instances, no reason for discipline. There may be reason to make sure our systems are fixed so that a technical violation, or technical error doesn't exist again because we've identified it. But nothing intentional.

LITT: Can I just add one thing to that point? An important part of the oversight process that the Department of Justice, and the ODNI engage in is when compliance problems are identified, and the vast majority of them are self-identified by NSA, but when a compliance issue is identified, we go and look at it and say, OK are there changes that need to be made in the system so that this kind of mistake doesn't happen again? It's a constantly improving process to prevent problems from occurring.

MILLER: Thank you. I yield back.

ROGERS: Ms. Schakowsky?

SCHAKOWSKY: Thank you Mr. Chairman. General Alexander, do you feel that this open hearing today jeopardizes in any way our national security?

ALEXANDER: I don't think the sharing itself jeopardizes it. I think the damage was done in the release of the information already. I think today what we have the opportunity is (sic) so where it makes sense, provide additional information on the oversight, the compliance and some of the -- the statistics, without jeopardizing it. So to answer your question, no. We're being very careful to do that, and I appreciate what the committee has done on that.

SCHAKOWSKY: How many people were in the same position as Snowden was, as a systems manager to have access to this information that could be damaging if released?
ALEXANDER: Well, there are system administrators throughout NSA and in our -- all our complexes around the world. And there is on the order of a thousand system administrators, people who actually run the networks that have, in certain sections, that -- that level of authority and ability to interface with...

SCHAKOWSKY: How many of those are outside contractors, rather than...

ALEXANDER: The majority are contractors. As you may know, as

you may recall, about 12-13 years ago as we tried to downsize our government work force, we pushed more of our information technology workforce or system administrators to the contract arena. That's consistent across the intelligence community.

SCHAKOWSKY: I would -- I would argue that this conversation that we're having now could have -- could have happened unlike what you said Mr. Litt. And perhaps we disagree also, General Alexander, that the erosion of trust, the misconceptions and the misunderstandings that resulted and why would assume that when there's 1,000 -- are there any more than 1,000 by the way?

ALEXANDER: Well, we're actually counting all of those positions. I'll get you an accurate number.

SCHAKOWSKY: That -- that some of this information would not have become public. And that the effort that has to convince the American public of the necessity of this program, I think would suggest that we would have been better off at having a discussion of vigorous oversight, the legal framework, et cetera up front, and how this could prevent perhaps another 9/11, and in fact, 50 or so, attacks. Let me ask you this, Mr. Cole, you know you -- you were talking about transparency, and you were saying that -- essentially that while the Verizon phone records order looked bad on its face, that there are other FISA court orders that talk in more depth about the legal rationale, about -- about what we're -- what we're doing.

So, will you release those court opinions with the necessary redactions, of course? And if not, why?

COLE: Well, I'm going to refer that over to Mr. Litt because the classifying authority on that would be DNI.

LITT: As you may know, we have been working for some time on trying to declassify opinions of the FISA court. It's been a very difficult task, because like most legal opinions, you have facts intermingled with legal discussion. And the facts frequently involve classified information, sensitive sources and methods. And what we've been discovering is that when you remove all of the information that needs to be classified, you're left with something that looks like Swiss cheese, and is not really very comprehensible. Having said that, I think as -- as General Alexander said, there's information out in the public domain now. There's -- the director of national intelligence declassified certain information about these programs last week.
And as a result of that, we are going back, taking another look at these opinions to see whether, in light of that declassification, there's now -- we can make a more comprehensible release of the opinion. So the answer to that is, we are looking at that and -- and frankly we would like to release it to the public domain, as much of this as we can, without compromising national security.

SCHAKOWSKY: I think -- General Alexander, so what other types of -- of records are collected under this Section 215? Can -- can you talk about that at all?

ALEXANDER: Yeah, for NSA the only -- the only records that are

collected under business records 215 is this telephony data. That's all.

SCHAKOWSKY: And is there authorization to collect more?

ALEXANDER: Under 215 for us? No, this is the only -- that we do. Now it gets into other authorities, but it's not ours. And I don't now if the -- I'll pass that to the attorney general because you're asking me now outside of NSA.

COLE: 215 is generally -- is a general provision that allows the acquisition of business records if its relevant to a national security investigation. So that showing has to be made to the court to allow that subpoena to issue that there is a relevance, and a connection. And that can be any -- any number of different kinds of records that a business might maintain; customer records, purchase orders, things of that nature. Somebody buys materials that they could buy an explosive out of, you could go to a company that sells those and get records of the purchase. Things of that nature.

SCHAKOWSKY: What about e-mails?

COLE: E-mails would not be covered by business records in that regard. You would have to -- under the Electronic Communications Privacy Act, you get specific court authorization for e-mails, that's stored content. If you're going to be looking at them in real time while they're going, you're going to have a separate FISA court order that would allow you to do that. It wouldn't be covered by the business records.

SCHAKOWSKY: Thank you Mr. Chairman.

ALEXANDER: Could I just make sure -- one clear part on the system administrator versus -- so what you get access to is helping to run the network, and the web servers that are on that network that are publicly available. To get to any data, like the business records 215 data that we're talking about, that's in an exceptionally controlled area. You would have to have specific certificates to get into that. I am not aware that he had -- he, Snowden, had any access to that. And on the reasonable articulable suspicion numbers and on what we're seeing there, I don't know of any inaccurate RAS numbers that have occurred since 2009.

There are rigorous controls that we have from a technical perspective that once the numbers can -- is considered RAS-approved, that you put that number in. You can't make a mistake because the system helps correct that now. So that -- that is a technical control that we have put in there.

SCHAKOWSKY: Thank you. I yield back.

CONAWAY: Well, thank you gentlemen. General Alexander thank you for your long service. Mr. Cole and Mr. Inglis went through -- through a very extensive array of the oversight and internal controls that are associated with -- with what's going on. In a business environment, Sarbanes-Oxley requires that companies go through their entire system to make sure that, not only do the details trees work,

but that the forest works as well. Is there any one at -- in the vast array of what you guys are doing that steps back and says, all right, we're -- the goal is to protect privacy and our civil liberties and we're doing the very best we can.

Is there a -- an internal control audit, so to speak that looks at the entire system that says, we've got the waterfront covered? And we're doing what we need to do?

COLE: I'll start. I mean there are these periodic reviews that I've described that audit everything that is done under both of these programs by both NSA and the Department of Justice, and the Office of the Director of National Intelligence, and we report to the court, and we report to Congress. So all of that is done looking at the whole program at the same time.

CONAWAY: I guess I -- Mr. Cole I'm looking at the -- the program of that. I understand that those pieces work really well, and that that's their design to -- to go at it and create the -- that kind of audit process. But is there an overall look at -- at everything that is done to say, we've got it all covered? Or -- and if we don't, and there are suggestions that we need to improve it, where do those suggestions get vetted? And have we had suggestions for improvement that we said, no, we don't need to do that?

LITT: Mr. Conaway if I might speak on that, there are at least two levels at which that takes place.

One is by statute within the Office of the Director of National Intelligence, there is -- there is a civil liberties protection officer -- his name is Alex Joel, who's an incredibly capable person whose job it is to take exactly that kind of look at our programs and make suggestions for the protection of civil liberties.

Outside of -- of the intelligence community, there...

(CROSSTALK)

CONAWAY: And that person would have the requisite clearances to know all the details?

(CROSSTALK)

LITT: Absolutely. He is -- he is, in fact, part of this audit process as well, his office is.

The second thing is that -- is that outside of the intelligence community, the president's Civil Liberties Oversight Board, which has -- has five confirmed members is also charged with evaluating the impact of our counterterrorism programs on privacy and civil liberties.

They also have full clearances. They have the ability to get full visibility into this program. In fact, they have recently been briefed on these programs, and I know they are, in fact, looking at them to make exactly that kind of assessment.

(CROSSTALK)

CONAWAY: And who -- who do they report to? Is that report public?

LITT: It's the president's board. I suspect that to the extent they're making a classified report, it would not be public. To the extent that they can make an unclassified report, it's up to them whether or not it becomes public.

CONAWAY: Several of you mentioned the term "minimization" and then also five-year destruction, rolling five-year window on the -- on the business record issues. You've used the word "purge," "get rid of," "destroy."
In an electronic setting, can you help us understand exactly what that means? I understand when I shred a piece of paper into the thousand-and-one pieces, that's one thing. But given the number of times you back up data and all the other, can a citizen feel like that once the minimization worked, that this electronically, we have in fact deleted all these things that are -- that we're supposed to delete?

INGLIS: So I'll start at that. Yes, sir, I believe that we can.
We have a fairly comprehensive system at NSA that whenever we collect anything, whether it's under this authority or some other, we actually bind to that communication where we got it, how we got it, what authority we got it under so that we know precisely whether we can retain it for some fixed period of time.

And if it simply ages off, as in the case of the B.R. FISA data we talked about, at the expiration of those five years, it is automatically taken out of the system. Literally just deleted from the system.

CONAWAY: OK. And it's mechanically overwritten and all of the back-up copies of that are done away with, and...

INGLIS: Yes, sir.

CONAWAY: OK.

INGLIS: It's -- it gets fairly complicated very quickly, but we have what are called source systems of record within our architecture, and those are the places that we say if it -- if the data element has the right to exist, it's attributable to one of those. And if it doesn't have the right to exist, you can't find it in there.

And we have very specific lists of information that determine what the provenance of data is, how long that data can be retained. We have on the other side of the coin purge lists that if we were authorized -- if we were required to purge something, that item would show up explicitly on that list. And we regularly run that against our data sets to make sure that we've checked and double-checked that those things that should be purged have been purged.

CONAWAY: All right.

One quick one: Any indication that the -- the FISA court has a problem with resources necessary to run its oversight piece?

INGLIS: Not that I'm aware of right now. But, obviously, the courts are suffering under sequestration, like everybody else. So I don't know what's gonna hit them as we go forward.

CONAWAY: Thank you, sir,

I yield back.

ROGERS: Mr. Conaway.

Mr. Langevin?

LANGEVIN: Thank you, Mr. Chairman.

And gentlemen, I want to thank you all for your testimony here today and for your service to our -- our country.

I'm -- as members of the committee, I have been briefed on the program, and -- and I know the excess of due diligence you've gone through to make sure that this is done right.

So I think it's important that this discussion is being had this morning. And hopefully it's gonna give greater confidence to the American people that all the agencies involved have dotted their i's and crossed their t's.

I especially think it's helpful that we have the discussion about the FISA court today and -- and how detailed the -- the requests have to be before they get approval and it's made clear that these are not just one-page documents that are presented to a FISA judge and then it's rubber stamped.

It actually goes through excessive due diligence, and -- and before it even gets to the point where the judge sees it. And, obviously, if the -- if all the criteria have been met, then it gets -- it gets approved, and if it's -- if the criteria have not been met, it's gonna be rejected.

So, I won't belabor that point, excepting that's been had -- been a very fruitful discussion.

But can you talk further about the -- again the role of the I.G. and go into that -- that -- that process a little more so that the -- the amount of review the I.G. does, once a query has been made in terms of the range of queries that have been made, I think that's -- would be important to clarify.

INGLIS: I would just start with that, and then defer to the ODNI and the attorney general -- deputy attorney general for some followup.

And so, at NSA, any analyst that wants to form a query, regardless of whether it's this -- this authority or any other, essentially has a two-person control rule. They would determine

whether this query should be applied, and there's someone who provides oversight on that.

We've already learned that under the metadata records that are captured by the B.R. FISA program, that there's a very special court-defined process by which that's done.

Those are all subject to the I.G., the inspector general's review on a periodic basis, such that we can look at the procedures as defined, the procedures as executed, reconcile the two and ensure that internal to NSA, that that's done exactly right. There are periodic reports that the I.G. has to produce on these various programs, and they are faithfully reported.
But I think the real checks and balances within the executive branch happen between NSA and the Department of Justice, the Office of the Director of National Intelligence. And because NSA also has a foot within the Department of Defense, the Department of Defense enters into that as well. They have intelligence oversight mechanisms.

And between those four components, there is rich and rigorous oversight which varies in terms of the things that they look for, based upon the authorities. B.R. FISA is a particularly rigorous authority. But they all have checks and balances to transcend just NSA.

LANGEVIN: OK.

COLE (?): And, Congressman, if I -- if I could add to that, and I refer you to a recent review by the DOJ inspector general on the 702 program that was highly complimentary of all the checks and balances that were in place.

LANGEVIN: Thank you.

So let me turn my attention now to -- I know these programs primarily target non-U.S. persons, but can you -- and this is probably a question for you, Mr. Joyce, just to clarify, you've said that if a U.S. person or a -- the overseas or the United States or a non-U.S. person living in the United States, that if they're -- we become aware that they may be involved in terrorist activity that they are served -- processed.

Can you go into that level of detail of what then happens and how the courts are involved with -- if we become aware that a U.S. person is involved?

JOYCE: So -- so I think either -- maybe I misspoke or -- or you misspoke. We -- we -- we are not looking at all at U.S. persons. The 702 is anyone outside the United States. And even if a U.S. person is outside of the United States, it does not include it in the 702 coverage.

OK, so it's a non-U.S. person outside the United States, and it has to have -- there's three different criteria it goes through. One of those links is terrorism. So that is where specifically only certain individuals are targeted. Those ones, one of the criteria,

linked to terrorism.

On numerous occasions, as I've outlined in some of the examples, those individuals outside the United States were discovered communicating with someone inside the United States.

We then -- that is, being tipped from the NSA. We then go through the legal process here, the FBI does, regarding that U.S. person. So we go and we have to serve what's called a national security letter to identify the subscriber. It's much like a subpoena.
Following that, if we want to pursue electronic surveillance, we have to make a specific application regarding that person with the FISA court here.

LANGEVIN: That's what I was looking for. So thank you very much.

I yield back.

(OFF-MIKE)

ALEXANDER: Sir, if I could, just to follow on and -- and to clarify, 'cause as we're going through this, I want to make sure that everything we say is exactly right -- from from my perspective. And so, as Sean said, NSA may not target the phone calls or e-mails of any U.S. person anywhere in the world without individualized court orders.

LANGEVIN (?): OK. Thank you.

ROGERS: That's an important point we can't make enough.

Mr. Lobiondo?

LOBIONDO: Thank you. Thank you, Mr. Chairman.

General Alexander and team, thank you for helping -- helping us understand in so many closed sessions and hopefully helping the nation understand what we're doing, why we're doing it, and how we're doing it.

I want to focus a little bit more on 702, if we could.

And, General Alexander, could you -- could you explain what happens if a target of surveillance is communicating with a U.S. person in the United States?

ALEXANDER: So, under 702, I think the best case is some that Sean Joyce made. If we see, if we're tracking a known terrorist in another country, say Pakistan, Yemen or someplace, and we see them communicating with someone in the United States, and it has a terrorism nexus, focused on doing something in the United States, we tip that to the FBI.

So our job is to identify, see the nexus of it. It could be in another country as well. So sometimes, we'd see somebody in that --

one of those countries planning something in Europe or elsewhere. We would then share that through intelligence meetings to those countries.

But when it comes into the United States, our job ends. We're the outside and we provide that to the inside FBI to take it from there. So they, then, take it and say, "Does this make sense?" They'll go up, as Sean explained, look at the process for getting additional information to see if this is a lead worth following.

LOBIONDO: And what does the government have to do if it wants to target a U.S. person under FISA when they're located abroad -- when they're not here? What -- what would be the process for the government?

COLE: That would be the -- a full package going to the FISA court, identifying that person; identifying the probable cause to believe that that person is involved in either terrorism or foreign intelligence activities; and indicating that we have then the request to the court to allow us to intercept their communications because we've made the showing that they're involved in terrorist or foreign intelligence activities.

So we'd have to make a formal application targeting that person specifically, whether they're inside or outside of the United States.

LOBIONDO: And what if you...

(CROSSTALK)

INGLIS: And, sir, if I might. And again, that could not be done under 702. There's a separate section of the Foreign Intelligence Surveillance Act that would allow that, but it would not be doable under 702.

LOBIONDO: And -- and what if you want to monitor someone's communication in the United States?
COLE: Same thing. Again, a different provision of FISA, but we would have to show that that person is in fact with probable cause involved in foreign terrorist activities or foreign intelligence activities on behalf of a terrorist organization or a foreign power. We'd have to lay out to the court all of those facts to get the court's permission to then target that person.

LOBIONDO: So, I just want to reemphasize that. You -- you have to specifically go to the FISA court and make your case as to why this information is necessary to be accessed.

COLE: That's correct.

LOBIONDO: And without that, you have no authority and cannot do it and do not do it.

COLE: That's correct.

LOBIONDO: OK. Thank you.

I yield back, Mr. Chairman.

ROGERS: Great. Thank you very much.

Mr. Schiff?

SCHIFF: Thank you, Mr. Chairman.

And thank you, gentlemen, for your work.

On the business records program, the general FISA court order allows you to get the metadata from the communications providers. Then when there are reasonable and articulable facts, you can go and see if one of the numbers has a match in the metadata.

On those 300 or so occasions when you do that, does that require separate court approval? Or does the general FISA court order allow you, when your analysts have the reasonable, articulable facts, to make that query? In other words, every time you make the query, does that have to be approved by the court?

COLE: We do not have to get separate court approval for each query. The court sets out the standard that must be met in order to make the query, in its order. And that's in the primary order. And then that's what we audit in a very robust way in any number of different facets through both executive branch and then give it to the court, and give it to the Congress.

So we're given that 90-day period with these parameters and restrictions to access it. We don't go back to the court each time.

SCHIFF: And does the court scrutinize after you present back to the court, "these are the occasions where we found reasonable articulable facts," do they scrutinize your basis for conducting those queries?

COLE: Yes, they do.

SCHIFF: General Alexander, I wanted to ask you. I raised this in closed session, but I'd like to raise it publicly as well. What are the prospects for changing the program such that rather than the government acquiring the vast amounts of metadata, the telecommunications retain the metadata, and then only on those 300 or so occasions where it needs to be queried, you're querying the telecommunications providers for whether they have those business records related to a reasonable articulable suspicion of foreign terrorist connection?

ALEXANDER: I think jointly the FBI and NSA are looking at the architectural framework of how we actually do this program and what are the advantages and disadvantages of doing each one. Each case, as you know from our discussions, if you leave it at the service providers, you have a separate set of issues in terms of how you actually get the information, then how you have to go back and get that information, and how you follow it on and the legal authority for them to compel them to keep these records for a certain period of time.

So what we're doing is we're going to look at that and come back to the director of national intelligence, the administration and then to you all, and give you recommendations on that for both the House and the Senate. I do think that that's something that we've agreed to look at and that we'll do. It's just going to take some time. We want to do it right.

And I think, just to set expectations, the -- the concern is speed in crisis. How do we do this? And so that's what we need to bring back to you, and then I think have this discussion here and let people know where we are on it.

Anything that you wanted to add?

SCHIFF: I would -- I would strongly encourage us to vigorously investigate that potential restructuring. Even though there may be attendant inefficiencies with it, I think that the American people may be much more comfortable with the telecommunications companies retaining those business records, that metadata, than the government acquiring it, even though the government doesn't query it except on very rare occasions.

ALEXANDER: So it may be something like that that we'd bring back and look at. So we are going to look at that. And we have already committed to doing that and we will do that, and go through all the details of that.

SCHIFF: Mr. Litt, I wanted to ask you about the FISA court opinions. This week, I'm going to be introducing the House companion to the bipartisan Merkley bill that would require disclosure of certain FISA court opinions, again, in a form that doesn't impair our national security.

I recognize the difficulty that you described earlier in making sure those opinions are generated in a way that doesn't compromise the programs. You mentioned that you're doing a review, and I know one's been going on for sometime. In light of how much of the programs have now been declassified, how soon do you think you can get back to us about whether you're going to be able to declassify some of those FISA court opinions?

LITT: I'm hesitant to answer any question that begins "how soon," partly because there are a lot of agencies with equities in this, partly because there's a lot else going on in this area. My time has not been quite as free-up to address this topic as I would have liked over the last week-and-a-half.

I can tell you that -- that I've asked my staff to work with the other agencies involved and try to press this along as quickly as possible. We're trying to identify those opinions where we think there's the greatest public interest in having them declassified, and start with those. And we'd like to push the process through as quickly as possible at this point.

SCHIFF: And I would just encourage in the last second that beyond the two programs at issue here, to the degree you can

declassify other FISA court opinions, I think it's in the public interest.

LITT: Yes, I think that's part of what we're doing.

SCHIFF: Thank you, Mr. Chairman.

COLE: Congressman Schiff, I just wanted to correct a little bit one of the things I said. The FISC does not review each and every reasonable, articulable suspicion determination. What does happen is they are given reports every 30 days in the aggregate. And if there are any compliance issues, if we found that it wasn't applied properly, that's reported separately to the court.

ROGERS: Do you have a followup?

SCHIFF: Thank you, Mr. Chairman. I just want to make sure I understood what you just said. A prior court approval is not necessary for a specific query. But when you report back to the court about how the order has been implemented, you do set out those cases where you found reasonable articulable facts and made a query. Do you set out those with specificity or do you just say "on 15 occasions, we made a query"?

COLE: It's more the latter -- the aggregate number where we've made a query. And if there's any problems that have been discovered, then we with specificity report to the court those problems.

SCHIFF: It may be worth considering providing the basis of the reasonable and articulable facts and having the court review that as a -- as a further check and balance. I'd just make that suggestion.

ROGERS: Mr. Cole, my understanding, though, is that every access is already preapproved; that the way you get into the system is court-approved. Is that correct?

COLE: That's correct.

The court sets out the standards which have to be applied to allow us to make the query in the first place. Then the application -- the implementation of that standard is reviewed by NSA internally at several levels before the actual implementation is done. It's reviewed by the Department of Justice. It's reviewed by the Office of the Director of National Intelligence. It's reviewed by the inspector general for the National Security Agency. So there's numerous levels of review of the application of this. And if there are any problems with those reviews, those are then reported to the court.

ROGERS: And -- and just to be clear, so if they don't follow the court-approved process, that would be a variation, that would have to be reported to the court?

COLE: That's correct.

ROGERS: OK. But you are meeting the court-approved process with every query?

COLE: That's correct.

INGLIS: And sir, if I might add to that that every one of those query is audited, those are all reviewed by the Department of Justice. Those are the reviews that we spoked about -- spoke about at 30 and 90 days. And there's a very specific focus on those that we believe are attributable to U.S. persons despite the fact that in (inaudible) FISA we don't know the identities of those persons. And so the court gets all of those reports.

SCHIFF: Thank you, Mr. Chairman.

I -- I just point out, all those internal checks are valuable, but they're still internal checks. And it may be worthwhile having the court, if not prospectively at least after the fact review those determinations.

Thank you, Mr. Chairman.

NUNES: Thank you, Mr. Chairman.

Mr. Cole, really what's happened here is that the totality of many problems within the executive branch has now tarnished the fine folks at the NSA and the CIA. And I just made a short list here, but, you know, right after Benghazi there was -- there's lies after Benghazi, four dead Americans. Fast and Furious, the Congress still is missing documents. We have dead Americans and dead Mexican citizens. You at least tapped into or got phone records from AP reporters, Fox News reporters, including from the House Gallery right here within this building.

Last week, as you know, A.G. Holder has been -- is being accused by the Judiciary Committee of possibly lying to the committee.

And then to top it all off, you have, you know, an IRS official who with other officials ran like a covert media operation on a Friday to help, you know, try to release documents to think that this would just go away about the release of personal data from U.S. citizens from the IRS.

So now -- you know, I understand when my constituents ask me, "Well, if the IRS is leaking personal data" -- General Alexander, this question's for you -- "how do I know for sure that the NSA and the -- and (inaudible) people that are trying to protect this country aren't leaking data?"

So Mr. -- Mr. Rogers asked the question about, you know, how do we know that -- that someone from the White House just can't go turn a switch and begin to listen to their phone conversations?

So General, I think if you could clarify the -- kind of the difference in what the people that are trying to protect this country are doing and what they go through, the rigorous standards. I think it would help, I think, fix this mess for the American people.

ALEXANDER: Thank you, Congressman.

I think the key -- the key facts here. When we disseminate data, everything that we disseminate and all the queries that are made into the database are 100 percent auditable. So they are audited by not only the analysts who's actually doing the job but the overseers that look and see, did he do that right or she do that right.

In every case that we have seen so far we have not seen one of our analysts willfully do something wrong like what you you just said. That's where disciplinary action would come in.

What I have to overwrite -- underwrite is when somebody makes an honest mistake. These are good people. If they transpose two letters in typing something in, that's an honest mistake. We go back and say, now how can we fix it? The technical controls that you can see that we're adding in help fix that. But is -- it is our intent to do this exactly right.

In that, one of the things that we have is tremendous training programs for our people that they go through. How to protect U.S. persons data? How to interface with the business record FISA? The roles and responsibilities under FAA 702. Everyone, including myself, at NSA has to go through that training to ensure that we do it right.

And we take that very seriously. I believe the best in the world at (ph) terms of protecting our privacy.
And I would just tell you, you know, the other thing that's sometimes confused here is that, "Well, then they're getting everybody else in the world." But our -- our approach is foreign intelligence -- you know, it's the same thing in Europe. We're not interested in -- in -- well, one, we don't have the time. And, two, ours is to protect our country and our allies. I think we do that better than anyone else.

Now, Chris, anything -- if you want to add to that?

INGLIS: No, I think that's exactly right. When somebody comes to work at NSA, just like elsewhere in the government, they take an oath to the Constitution not to NSA, not to some particular mission but to the Constitution and the entirety of that Constitution. Covers the issues importantly that we're discussing here today: national security and the protection of civil liberties. There's no distinction for us. They're all important.

NUNES: So I want to -- I want to switch gears a little bit here, General Alexander -- and perhaps this is a good question for Mr. Joyce. But I just find it really odd that right before the Chinese president comes to this country that all of these leaks happen and this guy has fled to -- to Hong Kong, this Snowden. And I'm really concerned that just -- the information that you presented us last week. This is probably gonna be the largest leak in American history -- and there's still probably more to come out. Can you just explain to the American people the seriousness of this leak and the damage -- you said earlier that it's damaged national security. Can you go into a few of those specifics?

JOYCE: Very -- no. Really, I can comment very little other than

saying it's and ongoing criminal investigation. I can tell you, as we've all seen, these are egregious leaks -- egregious. It has affected -- we are revealing in front of you today methods and techniques. I have told you, the examples I gave you, how important they have been. The first core Al Qaida plot to attack the United States post-9/11 we used one of these programs. Another plot to bomb the New York Stock Exchange, we used these programs. And now here we are talking about this in front of the world. So I think those leaks affect us.

NUNES: General?

ALEXANDER: It also -- it also affects our partnership with our allies, because the way it comes out -- and with industry. I mean, it's damaged all of those. Industry's trying to do the right thing, and they're compelled by the courts to do it. And we use this to also protect our allies and our interests abroad.

And so I think the way it's come out and the way it looks is that we're willfully doing something wrong when in fact we're using the courts, Congress and the administration to make sure that everything we do is exactly right. And as Chris noted, we all take an oath to do that, and we take that oath seriously.

NUNES: And in fact, just in closing here, Mr. Chairman, we know from the Mandiant report that came out that other governments are busy doing this and expanding their cyber warfare techniques. And I just want to say that, you know, it is so vital, as the chairman's pointed out many times, for the folks and the work that you're doing at NSA and all of your folks, how important that is to not only today's security but tomorrow's security.

So thank you for your service, General.

I yield back.

ROGERS: I -- I would just dispute the fact that other governments do it any -- any way, shape or form close to having any oversight whatsoever of their intelligence gathering programs.

Ms. Sewell?

SEWELL: Thank you, Mr. Chairman.

I also want to thank all of our witnesses today for your service to this country and for helping to maintain our national security.

I'd like to talk a little bit about the security practices. You've spent a lot of time really explaining to the American people the various levels of complexity in which you have judicial oversight and congressional oversight. How did this happen? How did a relatively low level administrator -- service systems administrator I think you said, General Alexander -- have classified information? And is it an acceptable risk?

I get that you have 1,000 or so system administrators. It is extremely frightening that you would go through such measures to do

the balancing act internally to make sure that we're balancing protection and security and -- and privacy, and yet internally in your own controls, there are system administrators that can go rogue. Is it an acceptable risk? How did it happen? And is there oversight to these system administrators?

ALEXANDER: Well, there is oversight. What we are now looking at is where that broke down and what happened. And that's gonna be part of the investigation that we're working with the FBI on.

I would just come back to 9/11. One of the key things was we went from the need to know to the need to share. And in this case, what the system administrator had access to is what we'll call the public web forums that NSA operates. And these are the things that talk about how we do our business, not necessarily what's been collected as a results of that; nor does it necessarily give them the insights of the training and the other issues that -- training and certification process and accreditation that our folks go through to actually do this.

ALEXANDER: So those are in separate programs that require other certificates to get into. Those are all things that we're looking at. You may recall that the intelligence community looked at a new information technology environment that reduces the number of system administrators.

If we could jump to that immediately, I think that would get us a much more secure environment and would reduce this set of problems. It's something that the DNI is leading and that we're supporting, as you know, across the community. I think that is absolutely vital to get to. And there are -- there are mechanisms that we can use there that will help secure this.

Please.

SEWELL: So the -- to be clear, Snowden did not have the certificates necessarily -- necessary to lead that public forum?

ALEXANDER: So each -- each set of data that we would have -- and, in this case, let's say the business records, FISA -- you have to have specific certificates -- because this is a cordoned off. So that would be extremely difficult for him -- you'd have to get up to NSA, get into that room.

Others require certificates for you to be working in this area to have that. It -- he would have to get one of those certificates to actually enter that area. Does that make sense? In other words, it's a key.

SEWELL: Well, I think that -- I would encourage us to figure out a way that we can declassify more information. I thank you for giving us two additional examples of -- of -- of terrorist attacks that we have thwarted because of these programs. But I think that providing us with as much information as you can on FISA courts' opinions -- how -- how that goes -- would help the American public de-mystify what we're doing here. I think that the examples -- the additional

examples that you gave today were great.

But I also am concerned that we have contractors doing -- I get that we cannot -- that there was a move at some point to -- to not have as many government employees, and so we sort of out-sourced it. But given the sensitivity of the information and the access, even for -- for relatively low-level employees, do you see that being a problem? And -- and how do we go about...

ALEXANDER: So we do have significant concerns in this area. And it is something that we need to look at. The mistakes of one contractor should not tarnish all the contractors because they do great work for our nation, as well. And I think we have to be careful not to throw everyone under the bus because of one person.

But you -- you raised two great points that I think we -- we will look at. One, how do we provide the oversight and compliance? And I talked to our technology director about the two-person control for system administrators to make any change. We are going to implement that. And I think, in terms of what we release to the public, I am for releasing as much as we can. But I want to weigh that with our national security, and I think that's what you expect. That -- that's what the American people...

SEWELL: Absolutely.

ALEXANDER: ... expect us. So that's where I need to really join that debate on this side to make sure that what we do is exactly right. I think on things like how we minimize data, how we run this program, the -- those kinds of things, I think we can -- we -- we're trying to be -- that's why Chris went through those great details.

I think those are things that the American people should know. Because what they find out is -- shoot, look at the oversight, the compliance, and the training that are people are going through. This is huge. This isn't some rogue operation that a group of guys up at NSA are running. This is something that have oversight by the committees, the courts, the administration in a 100 percent auditable process on a business record FISA.

You know, that's extraordinary oversight. And I think when the American people look at that, they say, "Wow, for less than 300 selectors, that amount of oversight --" and that's what we jointly agreed to do. I think that's tremendous.

SEWELL: I do too. I -- I -- I applaud the efforts. I just -- I think that, given the nature of this leak, you know, we don't want our efforts to be for naught, if, in fact, what happens is that the -- the leaks get the American people so concerned that they -- we roll back on these programs, and therefore increase our vulnerability as a nation. I think that all of us -- that's not in anyone's best interest.

Going back to sort of the difference between private contractors and government employees, is there a difference in the level of security clearance that...

ALEXANDER: Same level of security clearance and the same process for securing them.

SEWELL: OK.

Thank you. I yield back the rest of my time.

ROGERS: Thank you.

Mr. Westmoreland.
WESTMORELAND: Thank you, Mr. Chairman.

Mr. Cole, as Mr. Nunes had mentioned about some of the other things that have come out about leaks and so forth, could you -- because my constituents ask me the difference and maybe what the attorney general did in going to the court to -- on the Rosen case saying that he was an unindicted co-conspirator, because that was actually about a leak also. What type of process or internal review did y'all go over before you asked for those phones to be tapped? And, to make it perfectly clear, that was not in a FISA court. Is that correct?

COLE: Number one, that was not a FISA court. In the Rosen case, there were no phones being tapped. It was just to acquire a couple of e-mails. And there is a very, very robust system. It's set out in regulations that the Department of Justice follows of the kinds of scrubbing and review that must be done before any subpoena like that can be issued.

You have to make sure that you've exhausted all other reasonable avenues of investigation that -- that's done before you even get to the decision about whether or not such a -- a process should be used. You have to make sure that the information you're looking at is very, very tailored and only necessary -- truly necessary to be able to move the investigation forward in a significant way.

There has -- there are restrictions on what can be done with the information. And it goes through a very long process of review from the U.S. attorney's office through the United States attorney him or herself, into the, usually, the criminal division of the Justice Department, through the assistant attorney general of the criminal division, through the deputy attorney general's office and up, ultimately, to the attorney general signing it. It gets a lot of review before that's done under the criteria that we have in our guidelines and our CFR.

WESTMORELAND: So -- so the DOJ didn't -- because -- (inaudible) a security leak, the DOJ didn't contact the FBI or the NSA, or there was no coordination with that? It was strictly a DOJ criminal investigation?

COLE: Well, the FBI does criminal investigation with...

WESTMORELAND: I understand.

COLE: ... the Department of Justice. And they were contacted in that regard. But it was not part of the FISA process. It did not

involve the NSA.

WESTMORELAND: And I think that's what we need to be clear of, is...

COLE: Correct.

WESTMORELAND: ... that it was absolutely not part of the FISA -- process. And that is a lot more detailed and a lot more scrutinized as far as getting information than what this was. Is that correct?

COLE: Well, they're both very detailed and very scrutinized processes. They're -- they have different aspects to them. But they're both very unusually, frankly, detailed and scrutinized, both of those processes.

WESTMORELAND: Thank you.

And, General, going back to what Ms. Sewell had asked about the difference of clearance that you would have with a contractor or a government employee, when you have 1,000 different contractors -- I mean, I know the -- from my experience on having had one of my staff go through a security clearance, it's pretty -- it's a -- it's a pretty detailed operation. And I know that this gentleman had previously, I believe, heard that he had worked for the CIA. Had there been any further clearance given to this individual when he became a contractor after he left the employee of the CIA?

ALEXANDER: No additional clearance. He had what's needed to work at NSA or one of our facilities, the top secret special intelligence clearance. And that goes through a series of processes and reviews. The director of national intelligence is looking at those processes to make sure that those are all correct. And -- and he stated he's taken that on. We support that objective.

But to work at NSA, whether you're a contract, a government civilian, or a military, you have to have that same level of clearance.

WESTMORELAND: Does it bother you that this general had only been there for a short period of time? Or is there any oversight or review or whatever of the individuals are that carrying out this work? Is there any type of probation time or -- or anything? Because, you know, it seems that he was there a -- a very short period of time.

ALEXANDER: So he had worked in a couple of positions. He had just moved into the Booz Allen position in March. But he had worked in a information technology position for the 12 months preceding that at NSA Hawaii. So he'd actually been there 15 months. He moved from one contract to another.

WESTMORELAND: So would he have been familiar with these programs at his previous job?

ALEXANDER: Yes. And I believe that's where -- going out on what we call, the public classified web servers that help you understand

parts of NSA, that he gained some of the information, and -- and took some of that. I can't go into more detail.

LITT: Mr. Westmoreland, if I just might...

WESTMORELAND: Yes?

LITT: ... make one point there? When you say, would he have become familiar with these programs? I think part of the problem that we're having these days is that he wasn't nearly as familiar with these programs as he's portrayed himself to be. And thus -- this is what happens when somebody, you know sees a tiny corner of things and thinks that it gives them insight and viability into the program.

WESTMORELAND: Thank you. I yield back.

HIMES: Thank you Mr. Chairman and I too would like to thank the panel for appearing here today and for your service to the country. I think I've told each of you that in my limited time on this committee, I've been heartened by your competence, and by the competence of the agencies in which you work. I'll also add that I've seen nothing in the last week, week and a half to suggest that any of these programs that are being discussed, are operating in any way outside the law. And I would add that the controls that appear to be in place on these programs seem -- seem solid. I'll also say that I don't know that there's any way to do oversight without a posture of skepticism on the part of the overseers.

And so I hope you'll take my observations and questions in that spirit. And I'd like to limit my questions and observations purely to Section 215 and the Verizon disclosures, which quite frankly, trouble me. They trouble me because of the breadth and the scope of the information collection. They trouble me because I think this is historically unprecedented in the extent of the data that is being collected on potentially all American citizens. And the controls which you've laid out for us, notwithstanding, I think new (sic) for this country. We know that when a capability exists, there's a potential for abuse. Mr. Nunes ran through a lot of current issues going back to J. Edgar Hoover bugging the hotel rooms of Martin Luther King, to Nixon, to concerns around the IRS.

If a capability exists, from time to time it will be abused. And one of the things that I'm concerned about is this individual who I -- who's resume would I think make him -- make it unlikely that he would get an unpaid internship in my office, he had access to some of the most sensitive information that we have. And perhaps he could have, or someone like him, could have chosen a different path. Could have accessed phone numbers and -- though we spent a lot of time on the fact that you don't get names, we all know that with a phone number and Google, you can get a name pretty quickly.

He could have chosen to make a point about Congressman Himes making 2:00 am phone calls out of a bar in Washington. Or the CEO of Google making phone calls. Or anything really. Information that we hold to be private. So I guess -- I've got two questions. I guess I direct this one on 215 to Mr. Litt and then Mr. Cole. Where do we draw the line? So in other words, so long as the information is not

information to which I have a reasonable expectation of privacy under Maryland v. Smith and under Section 215 powers, where do we draw the line?

Could you, for example have video data? As I walk around Washington my -- I suppose that you could probably reconstruct my day with video that is captured on third-party cameras. Could you keep that in a way that is analogous to what you're doing with phone numbers? And again with all of the careful guards and what not, could you not reconstruct my day because I don't have a reasonable expectation of privacy around -- I know that's a hypothetical, but I'm trying to identify where the line is?

COLE: Well, I think the -- the real issue here is how it's accessed? What it can be used for? How you can actually...

HIMES: I -- I -- I'm stipulating that that system, even though we know it's not perfect, I'm stipulating that that system is perfect. And I'm asking, where is the limit as to what you can keep in the tank?

COLE: I -- I think some of it is a matter for the United States Congress to decide as policy matters, and the legislating that you do surrounding these acts, as to where you're going to draw those lines. Certainly the courts have looked at this and determined that under the statutes we have, there is a relevance requirement, and they're not just saying out of whole cloth you're allowed to gather these things. You have to look at it all together. And they're only saying that you can gather this volume under these circumstances, under these restrictions, with these controls. Without those circumstances and controls and restrictions, the court may well not have approved the orders under 215 to allow that collection to take place.

So you can't separate that out, one from the other and say, just the acquisition, what can we do? Because the acquisition comes together with the restrictions on access.

HIMES: And if those restrictions and controls are adequate, there's theoretically no restriction on your ability to store information on anything for which I do not have the reasonable expectation for privacy?

COLE: I'll refer back to NSA...

(CROSSTALK)

HIMES: Let me...

(CROSSTALK)

HIMES: ... I do have one more question.

(CROSSTALK)

HIMES: Yeah, this is the conversation -- I do have one more -- much more...

ALEXANDER: Can I...

HIMES: ... specific question.

ALEXANDER: ... can I hit...

HIMES: Yeah.

ALEXANDER: ... if I could. I'll ask for more time if I could, because I do think what you've asked is very important. So your question is, could somebody get out and get your phone number and see that you were at a bar last night? The answer is no. Because first in our system, somebody would have had to approve, and there's only 22 people that can approve, a reasonable articulable suspicion on a phone number. So first, that has to get input. Only those phone numbers that are approved could then be queried. And so you have to have one of those 22 break a law. Then you have to have somebody go in and break a law. And the system is 100 percent auditable, so it will be caught.

There is no way to change that. And so on that system, whoever did that would have broken the law. That would be willful. And then that person would be found by the court to be in violation of a court order, and that's much more serious. We have never had that happen.

HIMES: Yeah. No, I -- I thank you. I appreciate that, and I -- I sort of -- I think it's really important to explore these -- these bright lines about what you can keep and what you can't. Again, I don't see anything about the control systems that are troubling, but I do have one last quick question if the chairman will indulge me in. General, this is I guess for you and it's -- it's something that I asked you in closed session. As we weigh this, because obviously we're weighing security against privacy and what not, as we weigh this, I think it's really important that we understand exactly the national security benefit. And I limit myself to 215 here. 50 episodes. I don't think it's adequate to say that 702 and 215 authorities contributed to our preventing 50 episodes. I think it's really essential that you grade the importance of that contribution. The question I asked you, and -- and you can answer now, or I'd really like to get into this. How many of those 50 episodes would have occurred, but for your ability to use the Section 215 authorities as disclosed in the Verizon situation? How essential, not just contributing to, but how essential are these authorities to stopping which terrorist attacks?

ALEXANDER: OK. For clarity over 50. And in 90 percent of those cases FAA 702 contributed, and in 50 percent I believe they were critical. We will send that to the committee.

HIMES: This is 702 you're talking about?

ALEXANDER: This is 702.

HIMES: OK.

ALEXANDER: Now, shifting to the business record FISA, and I'll do a Mutt and Jeff here, I'm not sure which one I am. There's just

over 10 that had a domestic. And the vast majority...

HIMES: 10 of the 50 were section...

ALEXANDER: Just over 10.

(CROSSTALK)

HIMES: And how many would you say were critical.

ALEXANDER: No. No, you're...

HIMES: I'm sorry.

ALEXANDER: ... let me finish.

HIMES: Did I get it wrong?

ALEXANDER: Yeah, you do. Over -- just slightly over 10, and I don't want to pin that number until the community verifies it, so just a little over 10 were a domestic -- had a domestic nexus. And so business records FISA could only apply to those? So, see the ones in other countries, it couldn't apply to because the data is not there and it doesn't come into the U.S. So if we now look at that, the vast majority of those had a contribution by business record FISA. So, I think we have to be careful that you don't try to take the whole world and say, oh well you only did those that were in the United States and only, you know some large majority of that.

I do think this, going back to 9/11, we didn't have the ability to connect the dots. This adds one more capability to help us do that. And from my perspective, what we're doing here with the civil liberties and privacy oversight, and bringing together, does help connect those dots. Go ahead, Sean?
HIMES: If I could just -- I -- I'm out of time, but I think this point is really important. If my constituents are representative of the broader American public, they're more concerned frankly with the Section 215 gathering of American data than they are with the foreign data. And so I really hope you'll elucidate for us specifically case by case how many stopped terrorist attacks were those programs, 215, essential to?

JOYCE: I would just add to General Alexander's comments.

And I -- and I think you asked an almost impossible question to say, how important each dot was.

What I can tell you is, post 9/11 I don't recognize the FBI I came into 26 years ago. Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States. And I can tell you every tool is essential and vital. And the tools as I outlined to you and their uses today have been valuable to stopping some of those plots. You ask, "How can you put the value on an American life?" And I can tell you, it's priceless.

HIMES: Thank you, Mr. Chairman.

ROGERS: (OFF-MIKE)

BACHMANN: Thank you, Mr. Chair, for holding this important hearing today.

I just have a series of short questions. My first one is, you had mentioned earlier in your testimony that data must be destroyed within five years of acquisition. I believe that's in section 215 phone records. Is that -- that's true, within five years?

INGLIS: That is true. It's destroyed when it reaches five years of age.

BACHMANN: And how long do the phone companies on their own maintain data?

INGLIS: That varies. They don't hold that data for the benefit of the government. They hold that for their own business internal processes. I don't know the specifics. I know that it is variable. I think that it ranges from six to 18 months and the data that they hold is, again, useful for their purposes, not necessarily the government's.

BACHMANN: So then my question is, did the FISA orders give the United States companies a choice in whether to participate in the NSA business records or in the PRISM programs? Were these -- was this voluntarily -- voluntary compliance on the part of these companies?

INGLIS: No, these are court orders that require their compliance with the terms of the court order.

BACHMANN: So let me just for the record state, is NSA spying today or have you spied on American citizens?

INGLIS: We -- we do not target U.S. persons anywhere in the world without a specific court warrant.

BACHMANN: And does the NSA listen to the phone calls of American citizens?

INGLIS: We do not target or listen to the telephone calls of U.S. persons under that targeting without a specific court warrant.

BACHMANN: Does the NSA read the e-mails of American citizens?

INGLIS: Same answer, ma'am.

BACHMANN: Does the NSA read the text messages of American citizens?

INGLIS: Again, we do not target the content of U.S.-person communications without a specific warrant anywhere on the earth.

BACHMANN: Has the NSA ever tracked any political enemies of the administration, whether it's a Republican administration or Democrat administration? Have either of the administrations -- you said you're

100 percent auditable, so you would know the answer to this question -- have you ever tracked the political enemies of an administration?

INGLIS: In my time at NSA, no, ma'am.

BACHMANN: Does the government keep the video data, like Mr. Himes had just questioned? Does the government have a database with video data in it, tracking movements of the American people?

INGLIS: No, ma'am.

(CROSSTALK)

BACHMANN: I'm sorry. That's not -- the microphone isn't on.

INGLIS: NSA does not hold such data.

ALEXANDER: Yeah, and we don't know of any data -- anybody that does. So I think those are held, as you see from Boston, by individual shop owners and (inaudible).

BACHMANN: But -- but does the federal government have a database with video data in it tracking the whereabouts of the American people?

JOYCE: The FBI does not have such a database, nor am I aware of one.

BACHMANN: Do we -- does the American government have a database that has the GPS location whereabouts of Americans, whether it's by our cell phones or by any other tracking device? Is there a known database?

INGLIS: NSA does not hold such a database.
BACHMANN: Does the NSA have a database that you maintain that holds the content of Americans' phone calls? Do you have recordings of all of our calls? So if we're making phone calls, is there a national database that has the content of our calls?

ALEXANDER: We're not allowed to do that, nor do we do that, unless we have a court order to do that. And it would be only in specific cases and almost always that would be an FBI lead, not ours.

BACHMANN: So do we maintain a database of all of the e-mails that have ever been sent by the American people?

ALEXANDER: No. No, we do not.

BACHMANN: Do we -- is there a database from our government that maintains a database of the text messages of all Americans?

ALEXANDER: No -- none that I know of, and none at NSA.

BACHMANN: And so I think what you have told this committee is that the problem is not with the NSA, that is trying to keep the American people safe. You've told us that you have 100 percent auditable system that has oversight both from the court and from

Congress.

It seems to me that the problem here is that of an individual who worked within the system, who broke laws, and who chose to declassify highly sensitive classified information. It seems to me that's where our focus should be, on how there could be a betrayal of trust and how a traitor could do something like this to the American people. It seems to me that's where our focus must be and how we can prevent something like that from ever happening again.

Let me ask your opinion: How damaging is this to the national security of the American people that this trust was violated?

ALEXANDER: I think it was irreversible and significant damage to this nation.

BACHMAN:: Has this helped America's enemies?

ALEXANDER: I believe it has. And I believe it will hurt us and our allies.

BACHMANN: I yield back, Mr. Chair.

ROONEY: Thank you, Mr. Chairman.

I want to thank the panel.

You know, one of the negatives about being so low on the totem pole up here is basically all the questions that I wanted to address have been asked.

And I think I'm really proud of this committee because on both sides of the aisle, a lot of the questions were very poignant. And I hope that the American people and those that are in the room have learned a lot about what happened here and learned a lot about the people on the panel.

I can say specifically, General Alexander, my time on the Intelligence Committee, I have more respect for you. And I'm glad that you're the one up there testifying so the American people can see despite what they're -- what's being portrayed and the suspicions that are out there, that there is nobody better to articulate what happened and what we're trying to do than yourself.

So I want to thank you for that.

We -- we -- I'll ask a couple basic questions that I think that might help clear some things up.

Mr. Cole, you talked about how the -- the Fourth Amendment isn't applicable under the business records exception and the Patriot Act Section 215, applicable case law, Maryland v. Smith, et cetera. And then we heard about how to -- to be able to look at the data under 215, there has to be very specific suspicion that is presented to a court, and that court is not a rubber stamp in allowing us to basically look at metadata which is strictly phone records.

One of, I think, problems that people have out there is that it was such a large number of phone numbers. And when you testify, when everybody testifies, that it's very specific and only a limited number of people are able to -- to basically articulate who we should be looking at and then you hear this number, millions, from Verizon, can you -- can you help clear that up?

COLE: Certainly. First of all we -- as we said, we don't give the reasonable suspicion to the court ahead of time. They set out the standards for us to use.

But the analogy, and I've heard it used several times is, if you're looking for a needle in the haystack, you have to get the haystack first. And that's why we have the ability under the court order to acquire -- and the key word here is acquire -- all of that data.

We don't get to use all of that data necessarily. That is the next step, which is you have to be able to determine that there is reasonable, articulable suspicion to actually use that data.

So if we want to find that there is a phone number that we believe is connected with terrorist organizations and terrorist activity, we need to have the rest of the haystack, all the other numbers, to find out which ones it was in contact with.

And, as you heard Mr. Inglis say, it's a very limited number of times that we make those queries because we do have standards that have to be met before we can even make use of that data. So while it sits there, it is used sparingly.

ROONEY: Did you or anybody that you know at the NSA break the law in trying to obtain this information?

COLE: I am aware of nobody who has broken the law at the NSA in obtaining the information in the lawful sense. There's other issues that we have with the leaks that have gone on here.

ROONEY: And maybe this question is for General Alexander: Based on everything that we've heard today, do you see any problems with either 702 or 215 that you think should be changed by this body?
ALEXANDER: Not right now. But this is something that we have agreed that we would look at, especially the structure of how we do it.

I think Congressman Schiff brought up some key points, and we are looking at all of those. And what we have to bring back to you is the agility, how we do it in the oversight, is there other ways that we can do this.

But at the end of the day, we need these tools and we just got to figure out the right way to do it or the next step from my perspective, having the court, this body of Congress and the administration do oversight.

I think if the American people were to step through it, they would agree that what we're doing is exactly the right way.

ALEXANDER: So those are the steps that we will absolutely they'll go back and -- and look at the entire architecture and that's a commitment that FBI and NSA has made to the administration and to this committee.

ROONEY: Final question, Mr. Joyce, what's next for Mr. Snowden we can expect?

JOYCE: Justice.

ROONEY: I yield back, Mr. Chairman. Thank you.

(CROSSTALK)

POMPEO: Great. Thank you, Mr. Chairman.

Thank you all for being here today. You know, this has been -- this has been a great hearing. I think the American people will have gotten a chance to hear from folks who are actually executing this program in an important way, and they'll have a choice whether to believe Mr. Inglis and General Alexander or a felon who fled to communist China.

For me, there's an easy answer to that.

There are those who talk about the war on terror winding down, they say we're toward the end of this, these programs were created post-9/11 to counter the terrorist threat, but for the soldiers fighting overseas and our allies and for us in the States.

General Alexander, Mr. Joyce, do you think these programs are just as much needed today as they were in the immediate aftermath of 9/11?

ALEXANDER: I do.

JOYCE: I do, too. And I would just add, I think the environment has become more challenging. And I think the more tools you have to be able to fight terrorism, the more we're gonna be able to protect the American people.

POMPEO: Thank you.

We've talked a lot about the statutory basis for Section 215 and Section 702. We've talked a lot on all the process that goes with them. And I want to spend just a minute talking about the constitutional boundaries and where they are.

We've got FISA court judges, Article 3. Mr. Litt, these are just plain old Article 3 judges, in the sense of life time tenure, nominated by a president, confirmed by the United States Senate. They have the same power, restrictions and authority as all Article 3 judges do. Is that correct?

LITT: Yes, that's correct.

POMPEO: We have Article 2 before us here today and we've got Article 1 oversight taking place this morning.

I want to talk about Article 1's involvement. There have been some members who talked about the fact that they didn't know about these programs. General Alexander or maybe Mr. Inglis, can you talk about the briefings that you've provided for members of Congress, both recently and as this set of laws was developed -- set of laws were developed?

INGLIS: So 702 was recently reauthorized at the end of 2012. In the runup to that, NSA in the companionship with the Department of Justice, FBI, the DNI, made a series of presentations across the Hill some number of times and talked in very specific details at the classified level about the setup of those programs, the controls on those programs and the success of those programs.

The reauthorization of Section 215 of the Patriot Act came earlier than that, but there was a similar set of briefings along those lines.

At the same time, we welcome and continue to welcome any and all Congress persons or senators to come to NSA or we can come to you and at the classified level brief any and all details, That's a standing offer. And some number have, in fact taken us up on that offer.

POMPEO: Do you have something to add, General?

ALEXANDER: That's exactly right. In fact, anyplace, anytime we can help, we will do it.

POMPEO: Good. I appreciate that. I've been on the committee only a short time. I learned about these programs actually before I came on the committee, so I know that members outside of this committee also had access to the information. And I think that's incredibly important.

As -- as committee oversight members, that's one thing, but I think it's important that all the members of Congress understand the scope of these programs. And I appreciate the fact that you've continued to offer that assistance for all of us.

A couple of just clean-up details, going last. I want to make sure I have this right.

General Alexander, from the data under Section 215 that's collected, can you -- can you figure out the location of the person who made a particular phone call?

ALEXANDER: Not beyond the area code.

POMPEO: Do you have any information about the signal strength or tower direction? I've seen articles that talk about you having this information. I want to...

(CROSSTALK)

ALEXANDER: No, we don't.

POMPEO: ... we've got that right.

ALEXANDER: We don't have that in the database.

POMPEO: And then, lastly, Mr. Litt, you made a reference to Section 702. You talked about it being a restriction on Article 230, not an expansion. That is, Article 2, the presidents of both parties believed they had the -- the powers that are being exercised under Section 702 long before that statutory authority was granted.

So is it the case that you view Section 702 as a control and a restriction on Article 2?

LITT: Yes.

POMPEO: Great.

Mr. Chairman, I yield back.

(OFF-MIKE)

KING: Thank you, Mr. Chairman. I'll make this brief.

I want to first of all thank all witnesses for their testimony, for their service, and for all you've done to strengthen and maintain this program.

My question, General Alexander, is -- is to you and also perhaps to Mr. Joyce,

Several times in your testimony you referenced 9/11 and how -- and I recall after September 11th there was a -- was a loud challenge to the intelligence community to do a better job of connecting the dots, be more aggressive, be -- you know, be more forward thinking, try to anticipate what's going to happen, think outside the box, all those cliches we heard at the time.

And as I see it, this is a very legitimate and legal response to that request.

I would ask you, General Alexander, or you, Mr. Joyce, I believe referenced the case, after September 11th where there was a phone interception from Yemen which enabled you to foil the New York Stock Exchange plot,

It's also my understanding that prior to 9/11, there was phone messages from Yemen which you did not have the capacity to follow through on which perhaps could have prevented the 9/11 attack.

Could either General Alexander or Mr. Joyce or both of you explain how the attack could have been prevented? Or if you believe it could have been prevented?

JOYCE: I don't know, Congressman, if the attack could have been prevented. What I can tell you is that is a tool that was not

available to us at the time of 9/11. So when there was actually a call made from a known terrorist in Yemen to Khalid Mihdhar in San Diego, we did not have that tool or capability to track that call.

Now, things may have been different, and we will never know that, unfortunately.

So that is the tool that we're talking about today that we did not have at the time of 9/11.

Moving forward, as you mentioned about the -- the stock exchange, here we have a similar thing except this was under, again, the 702 program, where NSA tipped to us that a known extremist in Yemen was talking or conversing with an individual inside the United States, we later identified as Khalid Ouazzani.

And then we were able to go up on our legal authorities here in the United States on Ouazzani, who was in Kansas City and were able to identify two additional co-conspirators.

We found through electronic surveillance they were actually in the initial stages of plotting to bomb the New York Stock Exchange.

So, as -- to really summarize, as I mentioned before, all of these tools are important.

And as Congressman Schiff mentioned, we should have this dialogue. We should all be looking for ways, as you said, thinking outside the box of how to do our business.

But I sit here before you today humbly and say that these tools have helped us.

KING: General?

ALEXANDER: If I could, I think on Mihdhar case, Mihdhar was the terrorist -- the A.Q. terrorist from the 9/11 plot in California that was actually on American Airlines Flight 77 that crashed into the Pentagon -- what -- what we don't know going back in time is the phone call between Yemen and there, if we would have had the reasonable, articulable suspicion standard, so we'd have to look at that.

But assuming that we did, if we had the database that we have now with the business records FISA and we searched on that Yemen number and saw it was talking to someone this California, we could have then tipped that to the FBI.

Another step, and this an assumption, but let me play this out because we will never be able to go all the way back and redo all the figures from 9/11, but this is why some of these programs were put in was to help that.

Ideally going from Mihdhar, we would have been able to find the other teams, the other three teams in the United States and/or one in Germany or some other place.

So the ability to use the metadata from the business record FISA

would have allowed us, we believe, to see some.

Now, so it's hypothetical. There are a lot of conditions that we can put -- that we could put on there. You'd have to have this right. You'd have to have the RAS right.

But we didn't have that ability. We couldn't connect the dots because we didn't have the dots.

And so, I think what we've got here is that one additional capability, one more tool to help us work together as a team to stop future attacks. And as -- as Sean has laid out, you know, when you look at this, you know, the New York City -- two and others, I think from my perspective, you know, those would have been significant events for our nation. And so, I think what we've jointly done with Congress is helped set this program up correctly.

KING: I'll just close, General, by saying in your opening statement you said that you'd rather be testifying here today on this issue rather than explaining why another 9/11 happened.

So I want to thank you for your service in preventing another 9/11 and there's the Zazi case. And I know some -- you're very close with your knowledge of that. And I want to thank all of you for the effort that was done to prevent that attack.

Mr. Chairman, I yield back.

ROGERS: Just a couple of clarifying things here to -- to wrap it up.

Mr. Joyce, you've been in the FBI for 26 years. You've conducted criminal investigations as well.

Sometimes you get a simple tip that leads to a broader investigation. Is that correct?

JOYCE: That is correct, Chairman.

ROGERS: And so, without that initial tip, you might not have found the other very weighty evidence that happened subsequent to that tip. Is that correct?

JOYCE: Absolutely.

ROGERS: So, in the case of -- of Malalin (ph) in 2007, the very fact that under the business 215 records, there was a simple tip that was, we have someone that is known with ties to Al Qaida's east African network calling a phone number in San Diego. That's really all you got, was a phone number in San Diego. Is that correct?

JOYCE: That is correct.

ROGERS: And -- and according to -- in the unclassified report that tip ultimately led to the FBI's opening of a full investigation that resulted in the February 2013 conviction. Is that correct?

JOYCE: Yes, it is, Chairman.

ROGERS: So without that first tip, you would have had -- you -- you weren't up on his electronics communications. You didn't really -- you were not -- he was not a subject of any investigation prior to that tip from the National Security Agency.

JOYCE: No, actually, he was the subject to a prior investigation...

ROGERS: That was closed.

JOYCE: ... several years earlier that was closed...

ROGERS: Right.

JOYCE: ... because we could not find any connection to terrorism.

ROGERS: Right.

JOYCE: And then, if we did not have the tip from NSA, we would not have been able to reopen...

ROGERS: Reopen the case. But at the time, you weren't investigating him?

JOYCE: Absolutely not. It was based on...
(CROSSTALK)

ROGERS: Right, and when they -- when they dipped that number into the -- to the business records, the preserved business records from the court order -- they dipped a phone number in, and a phone number came out in San Diego. Did you know who that person was when they gave you that phone number?

JOYCE: No, we did not. So we had to serve legal process to identify that subscriber and then corroborate it. And then we later went up on electronic surveillance with an order through the FISC.

ROGERS: And -- and when you went up on the electronic surveillance, you used a court order, a warrant...

JOYCE: That is correct.

ROGERS: ... a subpoena? What did you use?

JOYCE: We used a FISA court order.

ROGERS: All right. So you had to go back. You had to prove a standard of probable cause to go up on this individual's phone number. Is that correct?

JOYCE: That's right. And as been mentioned, hopefully several times today, anyone inside the United States, a U.S. person, whether they're inside or outside, we need a specific court order regarding

that person.

ROGERS: All right.

And Mr. Cole, I just -- just for purposes of explanation, if you were going to have a -- an FBI agent came to you for an order to preserve business records, do they need a court order? Do they need a warrant for that in a criminal investigation?

COLE: No, they do not. You can just get a grand jury's subpoena, and, separate from preserving it, you can acquire them with a grand jury subpoena. And you don't need to go to a court to do that.

ROGERS: Right, so that is a lower-legal standard in order to obtain information on a U.S. citizen on a criminal matter.

COLE: That's correct, Mr. Chairman.

ROGERS: So the -- when we -- and I think this is an important point to make. When we -- the system is set up on this foreign collection -- and I argue we need this high standard because it is in a classified -- or used to be in a classified setting -- you need to have this high standard. So can you describe the difference?

If I were going to do a criminal investigation -- getting the same amount of information the -- the legal standard would be much lower if I were working an embezzlement case in Chicago than trying to catch a counter-terrorist -- counter -- excuse me, a terrorist operating overseas trying to get back into the United States to conduct a plot.

COLE: Some of the standards might be similar, but the process that you have to go through is much greater in the FISA context. You actually have to go to a -- a court, the FISA court ahead of time and set out facts that will explain to the court why this information is relevant to the investigation that you're doing, why it's a limited type of investigation that is allowed to be done under the statute and under the rules. And then the court has to approve that ahead of time, along with all of the rules and restrictions about how you can use it, how you can access it, what you can do with it, and who you can disseminate it to.

There is a much different program that goes on in a normal grand jury -- situation. You have restrictions on who you can disseminate to under secrecy grounds, but even those are much broader than they would be under the FISA grounds.

ROGERS: Right.

COLE: And you don't need a court ahead of time.

ROGERS: So -- so, in total, this is a much more overseen -- and, by the way, on a criminal embezzlement case in Chicago, you wouldn't brief that to Congress, would you?

COLE: No, we would not, not as a normal course.

ROGERS: Yeah, and so you have a whole nother layer of legislative oversight on this particular program. And, again, I argue the necessity of that because it is a -- as I said, used to be a classified program of which you additional oversight. You want members of the legislature making sure we're (ph) on track that you don't necessarily need in a criminal matter domestically.

COLE: That's correct. In a normal criminal embezzlement case in Chicago, you would have the FBI and the Justice Department involved. And that's about it.

ROGERS: Right.

COLE: In this, you've got the National Security -- Agency. You've got the ODNI. You've got the inspectors general. You've got the Department of Justice. You have the court monitoring what you're doing, if there's any mistakes that were made. You have Congress being briefed on a regular basis. There is an enormous amount of oversight in this compared to a grand jury situation. Yet the records that can be obtained are of the same kind.

ROGERS: Right, thanks. And I just want a couple of clarifying questions.

Mr. Joyce, if you will, does China have an -- an adversarial intelligence service directed at the United States?

JOYCE: Yes, they do.

ROGERS: Do they perform economic espionage activities targeted at U.S. companies in the United States?

JOYCE: Yes, they do.

ROGERS: Do they conduct espionage activities toward military and intelligent services, both here and abroad, that belong to the United States of America?

JOYCE: Yes, they do.

ROGERS: Do they target policy makers and decision makers, Department of State and other -- other policy makers that might engage in foreign affairs when it comes to the United States?

JOYCE: Yes.

ROGERS: Would you -- how would you rate them as an adversarial intelligence service given the other intelligence services that we know are adversarial, the Russians, the Iranians, the others?

JOYCE: They are one of our top adversaries.

ROGERS: Yeah. And you have had a string of successes recently in prosecutions for Chinese espionage activities in the United States. Is that correct?

JOYCE: That is correct.

ROGERS: And so, that has been both economic, and, if I understand it, as well as the military efforts. So they've been very aggressive in their espionage activities toward the United States. Is it -- would you -- is that a fair assessment?

JOYCE: I think they have been very aggressive against United States interests.

ROGERS: General Alexander, do they -- how would you describe, in an unclassified way, the Chinese cyber efforts for both espionage and their military capability to conduct disruptive attacks toward the United States?

ALEXANDER: Very carefully.

(LAUGHTER)

With a lot of legal oversight. I -- I think one of the things that -- you know, it's public knowledge out there about the cyber activities that we're seeing. But I also think that what's missing, perhaps, in this conversation with the Chinese is what's -- what's acceptable practices here. And I think the president has started some of that in the discussions with the -- the new president of China.

And I think that's some of the stuff that we actually have to have. This need not be an adversarial relationship. I think our country does a lot of business with China, and we need to look at, how can we improve the relations with China in such a way that both our countries benefit? Because we can. And I think that's good for everybody.

What concerns me is now this program and what we're talking about with China, as got -- I think we've got to solve this issue with China and then look at ways to move -- to move forward. And I think we do have to have that discussion on cyber. What is -- what are the right standards, have that discussion both privately and publicly. And it's not just our country. It's all the countries of the world, as well as China.

ROGERS: All right, and I -- I appreciate you drawing the line, but would you say that China engages in economic -- cyber economic espionage against intellectual property to steal intellectual property in the United States?

ALEXANDER: Yes.

ROGERS: Would you argue that they engage in cyber activities to steal both military and intelligence secrets of the United States?

ALEXANDER: Yes.

ROGERS: I -- I just -- I think this is important that we put it in context for several things that I think Americans want to know about the relationship between Mr. Snowden and -- and where he finds home today, and that we know that we're doing a full investigation

into possible connections with any nation state who might take advantage of this activity.

And the one thing I disagree with Mr. Litt today, that they haven't seen anything of any changes. And I would dispute that based on information I've seen recently and would ask anyone to comment. Do you believe that Al Qaida elements have -- have just historically, when they've been -- when issues have been disclosed, changed the way they operate to target both soldiers abroad in their terrorist-plotting activities, movements, financing, weaponization, and training.

LITT: To -- to be clear, what I -- what I intended to say -- and if I wasn't clear, I apologize -- was we know that they've seen this. We know they've commented on it. What we don't know yet is over the long term what impact it's going to have on our collection capabilities. But you're absolutely right. We know they watch us. And they -- they -- they modify their behavior based on what they learn.

ROGERS: And -- and we also know that in some cases in certain countries they have modified their behavior, including the way they target U.S. troops based on certain understandings of communications. Is that correct?

LITT: I think that's -- that's correct.

ROGERS: I'll guarantee it's absolutely correct. And that's what's so concerning about this.

I do appreciate your being here. I know how difficult it is to come and talk.

General, did you want to say something before...

(CROSSTALK)

ALEXANDER: Yeah, I -- I wanted to say, if I could, just a couple things, because they didn't come up in -- in this testimony. But, first, thanks to this committee, the administration and others, in the summer of 2009 we set up the director -- Directorate of Compliance. Put some of our best people in it to ensure that what we're doing is exactly right. And this committee was instrumental in helping us set that up. So that's one point.

When we talk about oversight and compliance, people think it's just once in a while, but there was rigorous actions by you and this entire committee to set that up.

The second is, in the open press there's this discussion about pattern analysis -- they're out there doing pattern analysis on this. That is absolutely incorrect. We are not authorized to go into the data, nor are we data mining or doing anything with the data other than those queries that we discuss, period. We're not authorized to do it. We aren't doing it. There are no automated processes running in the background pulling together data trying to figure out networks.

The only time you can do pattern analysis is, once you start the query on that query and where you go forward. You can't go in and try to bring up -- you know, I have four daughters and 15 grandchildren. I can't supervise them with this database. It is not authorized, and our folks do not do it.

And so that's some of the oversight and compliance you and the rest of the Oversight Committee see, but I think it's important for the American people to know that it's limited. In this case, for 2012, less than 300 selectors were looked at, and they had an impact in helping us prevent potential terrorist attacks, they contributed. And I think when you look at that and you -- you balance those two, that's pretty good.

ROGERS: And I do appreciate it. And I want to commend -- the folks from the NSA have always -- we've never had to issue a subpoena. All that information has always -- readily provided. You meet with us regularly. We have staff and investigators at the NSA frequently. We have an open dialogue when problems happen; we do deal with them in a classified way, in -- in a way I think that Americans would be proud that their elected representatives deal with issues.

And I'm not saying that there are some hidden issues out there; there are not.

I know this has been difficult to come and talk about very sensitive things in a public way. In order to preserve your good work and the work on behalf of all the patriots working to defend America, I still believe it was important to have a meeting where we could at least, in some way, discuss and reassure the level of oversight and redundancy of oversight on a program that we all recognize needed an extra care and attention and lots of sets of eyes. I hope today in this hearing that we've been able to do that.

I do believe that America has the responsibility to keep some things secret as we serve to protect this country. And I think you all do that well. And the darndest thing is that we may have found that it is easier for a systems analyst -- or a systems administrator to steal the information than it is for us to access the program in order to prevent a terrorist attack in the United States. And we'll be working more on those issues.

And we have had great dialogue about what's coming on some other oversight issues.

Again, thank you very, very much. Thank you all for your service. And I wish you all well today.

END

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

AMERICAN CIVIL LIBERTIES UNION, *et al.*, Plaintiffs, v. JAMES R. CLAPPER, Director of National Intelligence, *et al.*, Defendants.	13 Civ. 3994 (WHP) ECF Case

DECLARATION OF ACTING ASSISTANT DIRECTOR ROBERT J. HOLLEY
FEDERAL BUREAU OF INVESTIGATION

I, Robert J. Holley, here by state and declare as follows:

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

2. The FBI submits this declaration in the above-captioned case in support of the Government's opposition to the plaintiffs' motion for a preliminary injunction. The statements made herein are based on my personal knowledge, and information I have obtained in the course of carrying out my duties and responsibilities as Acting Assistant Director.

3. I discuss herein the National Security Agency's (NSA's) telephony metadata program, authorized by the Foreign Intelligence Surveillance Court (FISC) pursuant to Section

215 of the USA-PATRIOT Act, under which the NSA obtains and queries bulk telephony metadata for counterterrorism purposes. I address in unclassified terms the value of this program as a tool, including as a complement to other classified and unclassified FBI investigatory capabilities not discussed herein, for protecting the United States and its people from terrorist attack.

Overview of the NSA Telephony Metadata Program

4. One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. It is imperative that the United States Government have the capability to rapidly identify any terrorist threat inside the United States. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in this effort.

5. One method that the NSA has developed to accomplish this objective is the FISC-authorized bulk collection and analysis of telephony metadata that principally pertains to telephone calls to, from, or within the United States. Under the NSA's telephony metadata program authorized by the FISC, the term "metadata" refers to information that is about telephone calls but does not include cell site location information or the content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer. Specifically, such telephony metadata include comprehensive communications routing information, including but not limited to session identifying information *(e.g.,* originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of

call. By analyzing telephony metadata based on telephone numbers (or other identifiers) associated with terrorist operatives or activity, NSA analysts can work to determine whether known or suspected terrorists have been in contact with individuals in the United States. The NSA telephony metadata program was specifically developed to assist the Government in detecting communications between known or suspected terrorists who are operating outside of the United States and who are in contact with others inside the United States, as well as communications between operatives within the United States.

6. Under the NSA telephony metadata program at issue in this case, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores, queries, and analyzes the metadata for counterterrorism purposes. The FISC issues these orders under the "business records" provision of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act (Section 215). Under the terms of the FISC's orders, the authority to continue the program must be renewed every 90 days. The FISC first authorized the program in May 2006, and since then it has periodically renewed the program thirty-three times under orders issued by fourteen (14) different FISC judges.

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

metadata principally pertain to telephone calls made from foreign countries to the United States, calls made from the United States to foreign countries, and calls within the United States.

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

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

Court Approval

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

11. Starting in May 2006 fourteen (14) separate judges of the FISC have granted the Government's applications for bulk production of telephony metadata under this program on thirty-four (34) separate occasions. From time to time, prior to granting the Government's application the Court convenes a hearing to receive additional evidence and testimony regarding the program and its implementation (as occurred in connection with the most recent renewal of the program on July 19, 2013). On granting an application, the FISC issues a "Primary Order" that recites the court's findings, including that there are reasonable grounds to believe the call detail records sought are relevant to authorized FBI investigations to protect against international terrorism. The Primary Order then provides that certain telecommunications service providers, upon receipt of appropriate Secondary Orders (discussed below), shall produce to NSA on an ongoing daily basis for the duration of the Primary Order electronic copies of the call detail records created by them containing the "telephony metadata" discussed above, explicitly

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

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

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

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

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

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

15. Under the FISC Orders at issue, before NSA may query the metadata acquired under the FISC's orders for intelligence purposes, authorized NSA officials must determine that the identifiers on which the queries will be based are reasonably suspected of being associated with one (or more) of the foreign terrorist organizations specified in the Primary Order.

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

Investigative Value of Telephony Metadata to the FBI's Counter-Terrorism Mission

17. Counter-terrorism investigations serve important purposes beyond the ambit of routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, is to prevent terrorist attacks before they occur. Terrorism investigations also provide the basis for, and inform decisions concerning, other measures needed to protect the national security, including: excluding or removing persons involved in terrorism from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism; providing threat information and warnings to

other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism threats.

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

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

20. The NSA provides “tips” to the FBI regarding certain telephone numbers resulting from a query of the Section 215 telephony metadata. In certain instances, the FBI has received metadata-based tips containing information not previously known to the FBI about

domestic telephone numbers utilized by targets of pending preliminary investigations. The information from the metadata tips has provided articulable factual bases to believe that the subjects posed a threat to the national security such that the preliminary investigations could be converted to full investigations, which, in turn, led the FBI to focus resources on those targets and their activities. The FBI has also re-opened previously closed investigations based on information contained in metadata tips. In those instances, the FBI had previously exhausted all leads and concluded that no further investigation was warranted. The new information from the metadata tips was significant enough to warrant the re-opening of the investigations.

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

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

23. The tips or leads the FBI receives from bulk metadata analysis under this program can also act as an early warning of a possible threat to the national security. The sooner the FBI obtains information about particular threats to national security, the more likely it will be able to prevent and protect against them. Bulk metadata analysis sometimes provides information earlier than the FBI's other investigative methods and techniques. In those instances, the Section 215 NSA telephony metadata program acts as an "early warning system" of potential threats

against national security. Earlier receipt of this information may advance an investigation and contribute to the FBI preventing a terrorist attack that, absent the metadata tip, the FBI could not.

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

25. In October 2009, David Coleman Headley, a Chicago businessman and dual U.S. and Pakistani citizen, was arrested by the FBI as he tried to depart from Chicago O'Hare airport on a trip to Pakistan. At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the Prophet Mohammed. Headley was later charged with support to terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and put them in context with his U.S. based planning efforts.

26. In September 2009, using authorized collection under Section 702 to monitor al-Qa'ida terrorists overseas, NSA discovered that one of the al-Qa'ida associated terrorists was in

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

Alternatives to the NSA's Bulk Collection of Telephony Metadata

27. The NSA bulk collection program at issue here presents distinct advantages. The contact chaining capabilities offered by the program exceed the chaining that is performed on data collected pursuant to other means, including traditional means of case-by-case intelligence gathering targeted at individual telephone numbers such as subpoena, warrant, national security letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly defined orders under Section 215. This is so in at least two important respects, namely, the NSA's querying and analysis of the aggregated bulk telephony metadata under this program.

28. First, the agility of querying the metadata collected by NSA under this program allows for more immediate contact chaining, which is significant in time-sensitive situations of suspects' communications with known or as-yet unknown co-conspirators. For example, if investigators find a new telephone number when an agent of one of the identified international

terrorist organizations is captured, and the Government issues a national security letter for the call detail records for that particular number, it would only be able to obtain the first tier of telephone number contacts and, in rare instances, the second tier of contacts if the FBI separately demonstrates the relevance of the second-generation information to the national security investigation. At least with respect to the vast majority of national security letters issued, new national security letters would have to be issued for telephone numbers identified in the first tier, in order to find an additional tier of contacts. The delay inherent in issuing new national security letters would necessarily mean losing valuable time.

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

Conclusion

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

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

Executed on October 1, 2013.

Robert J. Holley
Acting Assistant Director
Counterterrorism Division
Federal Bureau of Investigation
Washington, D.C.