CASE NO. 15-16133

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, ERIC KNUTZEN, AND JOICE WALTON,

PLAINTIFFS-APPELLANTS,

V.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF CALIFORNIA, NO. 08-CV-04373-JSW
THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE, PRESIDING

APPELLANTS' EXCERPTS OF RECORD
Vol. 2 of 4, Pages ER 041 to ER 338

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
PHILIP J. TASSIN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
MARK RUMOLD
ANDREW CROCKER
JAMIE L. WILLIAMS
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Plaintiffs-Appellants

APPELLANTS' EXCERPTS OF RECORD

INDEX

(ECF Numbers are from N.D. Cal. No. 08-CV-04373-JSW.)

295	10/24/14	Declaration of Richard R. Wiebe in Support of Plaintiffs' Motion for Partial Summary Judgment	**ER 072**
288	9/29/14	[Redacted] Classified Declaration of Miriam P.	**ER 095**
286-3	9/29/14	Government Defendants' Opposition to Plaintiffs' Motion for Partial Summary Judgment and Cross-Motion for Partial Summary Judgment, Exhibit C (excerpt)	**ER 103**
265	7/25/14	Declaration of Joice Walton	**ER 106**
264	7/25/14	Declaration of Erik Knutzen	**ER 109**
263	7/25/14	Declaration of Carolyn Jewel	**ER 112**
262	7/25/14	Declaration of Richard R. Wiebe in Support of Plaintiffs' Motion for Partial Summary Judgment, Exhibits A, B (excerpt), C to F	**ER 115**
253-1, 253-3, 253-7	6/27/14	Declaration of James J. Gilligan in Support of Government Defendants' Reply Brief Regarding Compliance With Preservation Orders, Exhibits B, F	**ER 153**
203	3/24/14	Plaintiffs' Reply Re Question Three of the Court's Four Questions, Exhibit A	**ER 182**
161	9/30/13	Minute Order	**ER 191**
147	7/2/13	Declaration of Richard R. Wiebe in Opposition to the Government Defendants' Stay Request, Exhibit A (excerpts)	**ER 192**
114	10/9/12	Declaration of Cindy Cohn Pursuant to Fed. R. Civ. P. 56(d)	**ER 205**

CERTIFICATE OF SERVICE

I am over the age of 18 years, and not a party to this action. My business address is 815 Eddy Street, San Francisco, CA 94109, which is located in the county where the service described below took place.

I hereby certify that I electronically filed

APPELLANTS' EXCERPTS OF RECORD, Volumes 1, 2, and 4

with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on August 4, 2015.

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

On August 4, 2015, I served true and correct copies of the following document:

APPELLANTS' EXCERPTS OF RECORD, Volume 3 (Under Seal)

on the persons named below by placing copies in sealed envelopes, addressed as shown below, and mailing them, first class postage prepaid, to:

Douglas N. Letter
H. Thomas Byron III
Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice, Civil Division
950 Pennsylvania Ave., N.W.
Washington, DC 20530

Attorneys for United States defendants

James R. Whitman
Torts Branch
Civil Division, Room 8148
U.S. Department of Justice
1425 New York Ave., N.W.
Washington, DC 20005

Attorney for individual defendants

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

Dated: August 4, 2015

Stephanie Shattuck

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415/436-9333; Fax: 415/436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

PLAINTIFFS CAROLYN JEWEL, ERIK KNUTZEN AND JOICE WALTON'S NOTICE OF APPEAL AND REPRESENTATION STATEMENT

Courtroom 5, 2nd Floor
The Honorable Jeffrey S. White

Please take notice that plaintiffs Carolyn Jewel, Erik Knutzen and Joice Walton ("plaintiffs-appellants") hereby appeal to the United States Court of Appeals for the Ninth Circuit from the district court's judgment entered in this action pursuant to Federal Rule of Civil Procedure 54(b) on May 21, 2015 (ECF No. 328) and the district court's earlier order on which the judgment is based (ECF No. 321), which granted partial summary judgment to the government entity and official-capacity defendants and denied plaintiffs-appellants' motion for partial summary judgment, and all prior interlocutory rulings that are merged into the district court's judgment.

Plaintiffs-appellants' Representation Statement is attached to this Notice as required by Ninth Circuit Rule 3-2(b).

Dated: June 4, 2015

Respectfully submitted,

/s/ Andrew Crocker

ANDREW CROCKER
CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
DAVID GREENE
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
ROYSE LAW FIRM

RACHAEL E. MENY
MICHAEL S. KWUN
BENJAMIN W. BERKOWITZ
AUDREY WALTON-HADLOCK
JUSTINA K. SESSIONS
PHILIP J. TASSIN
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs

REPRESENTATION STATEMENT

Plaintiffs-appellants submit this Representation Statement pursuant to Rule 12(b) of the Federal Rules of Appellate Procedure and Ninth Circuit Rule 3-2(b). The counsel for plaintiffs designated below represent plaintiffs-appellants Carolyn Jewel, Erik Knutzen and Joice Walton. The counsel for plaintiffs designated below also represent plaintiffs who are not appellants for purposes of this appeal: Tash Hepting and Young Boon Hicks, as executrix of the estate of Gregory Hicks. The following list identifies all parties to the action, and it identifies their respective counsel by name, address, telephone number and email where appropriate.

PARTIES	COUNSEL OF RECORD
Plaintiffs-appellants Carolyn Jewel, Erik Knutzen and Joice Walton; additional plaintiffs in District Court Tash Hepting and Young Boon Hicks, as executrix of the estate of Gregory Hicks	DAVID GREENE (SBN 160107) davidg@eff.org CINDY COHN (SBN 145997) LEE TIEN (SBN 148216) KURT OPSAHL (SBN 191303) JAMES S. TYRE (SBN 083117) MARK RUMOLD (SBN 279060) ANDREW CROCKER (SBN 291596) ELECTRONIC FRONTIER FOUNDATION 815 Eddy Street San Francisco, CA 94109 Telephone: (415) 436-9333 Fax: (415) 436-9993 RICHARD R. WIEBE (SBN 121156) wiebe@pacbell.net LAW OFFICE OF RICHARD R. WIEBE One California Street, Suite 900 San Francisco, CA 94111 Telephone: (415) 433-3200 Fax: (415) 433-6382 RACHAEL E. MENY (SBN 178514) rmeny@kvn.com MICHAEL S. KWUN (SBN 198945) AUDREY WALTON-HADLOCK (SBN 250574) BENJAMIN W. BERKOWITZ (SBN 244441) JUSTINA K. SESSIONS (SBN 270914) PHILIP J. TASSIN (SBN 287787) KEKER & VAN NEST, LLP 633 Battery Street San Francisco, CA 94111 Telephone: (415) 391-5400

	Fax: (415) 397-7188 THOMAS E. MOORE III (SBN 115107) tmoore@rroyselaw.com ROYSE LAW FIRM, PC 1717 Embarcadero Road Palo Alto, CA 94303 Telephone: (650) 813-9700 Fax: (650) 813-9777 ARAM ANTARAMIAN (SBN 239070) aram@eff.org LAW OFFICE OF ARAM ANTARAMIAN 1714 Blake Street Berkeley, CA 94703 Tel.: (510) 289-1626
Attorneys for Government Defendant-Appellee Entities and Official-Capacity Individuals: National Security Agency, Department of Justice, United States of America, Barack Obama, Michael S. Rogers, Loretta E. Lynch, James R. Clapper, Jr.	ANTHONY J. COPPOLINO tony.coppolino@usdoj.gov Deputy Branch Director JAMES J. GILLIGAN Special Litigation Counsel RODNEY PATTON Trial Attorney JULIA BERMAN Trial Attorney MARCIA BERMAN Senior Trial Counsel PAUL GERALD FREEBORNE Attorney U.S. Department of Justice, Civil Division 20 Massachusetts Avenue, N.W. Room 6102 Washington, DC 20530 Tel: (202) 514-4782 Fax: (202) 616-8470
Attorneys for Government Defendants in their Personal Capacities: Keith B. Alexander, Michael V. Hayden, George W. Bush, Richard B. Cheney, David S. Addington, Alberto R. Gonzales, John D. Ashcroft, John M. McConnell, John D. Negroponte, Michael Mukasey,	JAMES R. WHITMAN U.S. Department of Justice 1425 New York Ave., N.W. Washington, DC 20005 202-616-4169 Fax: 202-416-4314 Email: james.whitman@usdoj.gov

Dated: June 4, 2015

Respectfully submitted,

/s/ Andrew Crocker
ANDREW CROCKER
CINDY COHN
LEE TIEN

KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
DAVID GREENE
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
ROYSE LAW FIRM

RACHAEL E. MENY
MICHAEL S. KWUN
BENJAMIN W. BERKOWITZ
AUDREY WALTON-HADLOCK
JUSTINA K. SESSIONS
PHILIP J. TASSIN
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415/436-9333; Fax: 415/436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

PLAINTIFFS' NOTICE OF ADDITIONAL AUTHORITIES

Date: December 19, 2014
Time: 9:00 a.m.
Courtroom 5, 2nd Floor
The Honorable Jeffrey S. White

Pursuant to the Court's December 16, 2014 Order (ECF No. 309), plaintiffs submit the following attached authorities on which they intend to rely at the December 19, 2014 hearing on the parties' cross-motions for partial summary judgment.

Exhibit A: Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014), pages 5-6, 16-20, 32, and 38-41;

Exhibit B: *Hearst v. Black*, 87 F.2d 68 (D.C. Cir. 1936), at pages 70-71;

Exhibit C: *United States v. Fowlkes*, 770 F.3d 748 (9th Cir. 2014), at pages 756-57; and

Exhibit D: *Coolidge v, New Hampshire*, 403 U.S. 443 (1971), at pages 454-55.

Dated: December 17, 2014

Respectfully submitted,

/s/ Richard R. Wiebe
RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
ANDREW CROCKER
DAVID GREENE
ELECTRONIC FRONTIER FOUNDATION

THOMAS E. MOORE III
ROYSE LAW FIRM

RACHAEL E. MENY
MICHAEL S. KWUN
BENJAMIN W. BERKOWITZ
AUDREY WALTON-HADLOCK
JUSTINA K. SESSIONS
PHILIP J. TASSIN
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs

Exhibit A

Exhibit A

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

Part 2:

EXECUTIVE SUMMARY

In 2008, Congress enacted the FISA Amendments Act, which made changes to the Foreign Intelligence Surveillance Act of 1978 ("FISA"). Among those changes was the addition of a new provision, Section 702 of FISA, permitting the Attorney General and the Director of National Intelligence to jointly authorize surveillance conducted within the United States but targeting only non-U.S. persons reasonably believed to be located outside the United States. The Privacy and Civil Liberties Oversight Board ("PCLOB") began reviewing implementation of the FISA Amendments Act early in 2013, shortly after the Board began operations as an independent agency.[9] The PCLOB has conducted an in-depth review of the program now operated under Section 702, in pursuit of the Board's mission to review executive branch actions taken to protect the nation from terrorism in order to ensure "that the need for such actions is balanced with the need to protect privacy and civil liberties."[10] This Executive Summary outlines the Board's conclusions and recommendations.

I. Overview of the Report

A. Description and History of the Section 702 Program

Section 702 has its roots in the President's Surveillance Program developed in the immediate aftermath of the September 11th attacks. Under one aspect of that program, which came to be known as the Terrorist Surveillance Program ("TSP"), the President authorized interception of the contents of international communications from within the United States, outside of the FISA process. Following disclosures about the TSP by the press in December 2005, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court ("FISA court") to conduct, under FISA, the collection that had been occurring under the TSP. Later, the government developed a statutory framework specifically designed to authorize this collection program. After the enactment and expiration of a temporary measure, the Protect America Act of 2007, Congress passed the FISA Amendments Act of 2008, which included the new Section 702 of FISA. The statute

---

9 *See* Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, *available at* http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf.

10 42 U.S.C. § 2000ee(c)(1).

provides a procedural framework for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance targeting persons who are not U.S. persons, and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, in order to acquire foreign intelligence information. Thus, the persons who may be targeted under Section 702 cannot intentionally include U.S. persons or anyone located in the United States, and the targeting must be conducted to acquire foreign intelligence information as defined in FISA. Executive branch authorizations to acquire designated types of foreign intelligence under Section 702 must be approved by the FISA court, along with procedures governing targeting decisions and the handling of information acquired.

Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired in a variety of ways. An example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is termed "incidental" collection. Another example is when two non-U.S. persons discuss a U.S. person. Communications of or concerning U.S. persons that are acquired in these ways may be retained and used by the government, subject to applicable rules and requirements. The communications of U.S. persons may also be collected by mistake, as when a U.S. person is erroneously targeted or in the event of a technological malfunction, resulting in "inadvertent" collection. In such cases, however, the applicable rules generally require the communications to be destroyed.

Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISA court the particular non-U.S. persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the "traditional" FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information. The certifications that have been authorized include information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.

Section 702 requires the government to develop targeting and "minimization" procedures that must satisfy certain criteria. As part of the FISA court's review and approval of the government's annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that

Part 3:

DESCRIPTION AND HISTORY

I. Genesis of the Section 702 Program

As it exists today, the Section 702 program can trace its lineage to two prior intelligence collection programs, both of which were born of counterterrorism efforts following the attacks of September 11, 2001. The first, and more well-known, of these two efforts was a program to acquire the contents of certain international communications, later termed the Terrorist Surveillance Program ("TSP"). In October 2001, President George W. Bush issued a highly classified presidential authorization directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States, based upon a finding that an extraordinary emergency existed because of the September 11 attacks. Under this authorization, electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.[16] President Bush authorized the NSA to (1) collect the contents of certain international communications, a program that was later referred to as the TSP, and (2) collect in bulk non-content information, or "metadata," about telephone and Internet communications.[17] The acquisition of telephone metadata was the forerunner to the Section 215 calling records program discussed in a prior report by the Board.

The President renewed the authorization for the NSA's activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court ("FISC" or "FISA court") were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President's Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, "the program

---

16 *See* DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) ("Dec. 21 DNI Announcement"), *available at* http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the.

17 *See* Dec. 21 DNI Announcement, *supra*.

became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."[18]

In December 2005, the *New York Times* published articles revealing the TSP, i.e., the portion of the President's Surveillance Program that involved intercepting the contents of international communications. In response to these revelations, President Bush confirmed the existence of the TSP,[19] and the Department of Justice issued a "white paper" outlining the legal argument that the President could authorize these interceptions without obtaining a warrant or court order.[20] Notwithstanding this legal argument, the government decided to seek authorization under the Foreign Intelligence Surveillance Act ("FISA") to conduct the content collection that had been occurring under the TSP.[21] In January 2007, the FISC issued orders authorizing the government to conduct certain electronic surveillance of telephone and Internet communications carried over listed communication facilities where, among other things, the *government* made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States.[22]

The FISC's order, referred to as the "Foreign Telephone and Email Order," in effect replaced the President's authorization of the TSP, and the President made no further reauthorizations of the TSP.[23] When the government sought to renew the January 2007 Foreign Telephone and Email Order, however, a different judge on the FISC approved the program, but on a different legal theory that required changes in the collection program.[24] Specifically, in May 2007 the FISC approved a modified version of the Foreign Telephone and Email Order in which the *court*, as opposed to the *government*, made probable cause determinations regarding the particular foreign telephone numbers and email addresses that were to be used to conduct surveillance under this program.[25] Although the modified

---

18 *See* UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, PREPARED BY THE OFFICE OF INSPECTORS GENERAL OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY, AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, at 31 (2009).

19 *See, e.g.*, President's Radio Address (Dec. 17, 2005), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html.

20 Legal Authorities Supporting the Activities of the National Security Agency Described by the President (January 19, 2006), *available at* http://www.justice.gov/olc/opiniondocs/nsa-white-paper.pdf.

21 *See* Dec. 21 DNI Announcement, *supra*.

22 Declassified Certification of Attorney General Michael B. Mukasey, at ¶ 37, *In re National Security Agency Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008) ("2008 Mukasey Decl."), *available at* http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf.

23 2008 Mukasey Decl., *supra*, at ¶ 37.

24 2008 Mukasey Decl., *supra*, at ¶ 38 & n.20.

25 2008 Mukasey Decl., *supra*, at ¶ 38.

Foreign Telephone and Email Order permitted the government to add newly discovered telephone numbers and email addresses without an individual court order in advance,[26] the government assessed that the restrictions of the order, particularly after the May 2007 modifications, was creating an "intelligence gap."[27]

Separate from, but contemporaneous with, the TSP and the Foreign Telephone and Email Orders, a second collection effort was being undertaken. Specifically, the government used the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers.[28] The government stated that it and the Foreign Intelligence Surveillance Court (FISC) expended "considerable resources" to obtain court orders based upon a probable cause showing that these overseas individuals met the legal standard for electronic surveillance under FISA,[29] i.e., that the targets were agents of a foreign power (such as an international terrorist group) and that they used the specific communication facilities (such as email addresses) regarding which the government was seeking to conduct electronic surveillance.[30] The persons targeted by these efforts were located outside the United States, and the communications being sought were frequently with others who were also located outside the United States.[31]

Drafting applications that demonstrated satisfaction of this probable cause standard, the government has asserted, slowed and in some cases prevented the acquisition of foreign intelligence information.[32] The government has not disclosed the scale of this second effort to target foreign individuals using traditional FISA electronic surveillance authorities, but in the years following the passage of the Protect America Act of 2007 and the FISA Amendments Act of 2008, which eliminated the requirement for the

---

26 2008 Mukasey Decl., *supra*, at ¶ 38.

27 *See* S. Rep. No. 110-209, at 5 (2007) (stating that "the DNI informed Congress that the decision . . . had led to degraded capabilities"); Eric Lichtblau, James Risen, and Mark Mazzetti, *Reported Drop in Surveillance Spurred a Law*, NEW YORK TIMES (Aug. 11, 2007) (reporting on Administration interactions with Congress that led to the enactment of the Protect America Act, including reported existence of an "intelligence gap").

28 Statement of Kenneth L. Wainstein, Assistant Attorney General, *Senate Select Committee on Intelligence Hearing On Modernization of the Foreign Intelligence Surveillance Act*, at 6-7 (May 1, 2007) ("May 2007 Wainstein Statement"), *available at* http://www.intelligence.senate.gov/070501/wainstein.pdf.

29 May 2007 Wainstein Statement, *supra*, at 6-7.

30 50 U.S.C. § 1805(a)(2).

31 May 2007 Wainstein Statement, *supra*, at 7.

32 *See, e.g.,* May 2007 Wainstein Statement, *supra*, at 7.

government to seek such individual orders, the total number of FISA electronic surveillance applications approved by the FISC dropped by over forty percent.[33]

In light of the perceived growing inefficiencies of obtaining FISC approval to target persons located outside the United States, in the spring of 2007 the Bush Administration proposed modifications to FISA.[34] Reports by the Director of National Intelligence to Congress that implementation of the FISC's May 2007 modifications to the Foreign Telephone and Email Order had resulted in "degraded" acquisition of communications, combined with reports of a "heightened terrorist threat environment," accelerated Congress' consideration of these proposals.[35] In August 2007, Congress enacted and the President signed the Protect America Act of 2007,[36] a legislative forerunner to what is now Section 702 of FISA. The Protect America Act was a temporary measure that was set to expire 180 days after its enactment.[37]

The government transitioned the collection of communications that had been occurring under the Foreign Telephone and Email Orders (previously the TSP) and some portion of the collection targeting persons located outside the United States that had been occurring under individual FISA orders to directives issued under the Protect America Act.[38] The Protect America Act expired in February 2008,[39] but existing Protect America Act certifications remained in effect until they expired.[40]

Shortly after passage of the Protect America Act, efforts began to replace it with a more permanent statute.[41] After substantial debate, in July 2008 Congress enacted and President Bush signed into law the FISA Amendments Act of 2008.[42] The FISA Amendments

---

33 *Compare* 2007 ANNUAL FISA REPORT (2,371 Title I FISA applications in 2007), *available at* http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf *with* 2009 ANNUAL FISA REPORT (1,329 Title I FISA applications in 2009), *available at* http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

34 *See* S. Rep. No. 110-209, at 2, 5 (noting Administration's submission of proposed modifications in April 2007); *see generally* May 2007 Wainstein Statement, *supra*; Statement of J. Michael McConnell, Director of National Intelligence, Before the Senate Select Committee on Intelligence (May 1, 2007), *available at* http://www.intelligence.senate.gov/070501/mcconnell.pdf.

35 *See* S. Rep. No. 110-209, at 5.

36 Pub. L. No. 110-55; 121 Stat. 552 (2007) ("Protect America Act").

37 Protect America Act § 6(c).

38 2008 Mukasey Decl., *supra*, at ¶ 13 & n.22.

39 *See* Protect America Act—Extension, Pub. L. No. 110-182, 122 Stat. 605 (2008) (extending Protect America Act for two weeks).

40 Protect America Act § 6.

41 *See, e.g.*, Press Release, The White House, President Bush Discusses the Protect America Act of 2007 (Sept. 19, 2007), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070919.html; S. Rep. No. 110-209, at 5.

42 Pub L. No. 110-261, 122 Stat. 2436 (2008).

Act replaced the expired Protect America Act provisions with the new Section 702 of FISA. The authorities and limitations of Section 702 are discussed in detail in this Report. In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which required judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information.[43]

After passage of the FISA Amendments Act, the government transitioned the collection activities that had been conducted under the Protect America Act to Section 702.[44] Section 702, as well as the other provisions of FISA enacted by the FISA Amendments Act, were renewed in December 2012, and are currently set to expire in December 2017.[45]

II. Statutory Structure: What Does Section 702 Authorize?

The Foreign Intelligence Surveillance Act is a complex law, and Congress' authorization of surveillance under Section 702 of FISA is no exception. In one sentence, the statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.[46] Each of these terms is, to various degrees, further defined and limited by other aspects of FISA. Congress also imposed a series of limitations on any surveillance conducted under Section 702. The statute further specifies how the Attorney General and Director of National Intelligence may authorize such surveillance, as well as the role of the FISC in reviewing these authorizations. This section describes this complex statutory framework.

A. Statutory Definitions and Limitations

Our description of Section 702's statutory authorization begins by breaking down the four-part sentence above.

First, Section 702 authorizes the *targeting of persons*.[47] FISA does not define what constitutes "targeting," but it does define what constitutes a "person." Persons are not only

---

43 50 U.S.C. §§ 1881b, 1881c.

44 2008 Mukasey Decl., *supra*, at ¶ 40 & n.22.

45 FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

46 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi).

47 50 U.S.C. § 1881a(a).

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers' assistance in the acquisition.[109] Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC.[110] The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government's acquisition of foreign intelligence information.[111] The FISC's decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.[112]

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number.[113] Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are *targeted*; selectors (e.g., email addresses, telephone numbers) are *tasked*. The users of any tasked selector are

---

109 50 U.S.C. § 1881a(h).

110 50 U.S.C. § 1881a(h)(4).

111 50 U.S.C. § 1881a(h)(5).

112 50 U.S.C. § 1881a(h)(6). However, as noted in the Board's Section 215 report, to date, only two cases have been appealed to the FISCR. One, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

113 *See* AUGUST 2013 JOINT ASSESSMENT, *supra*, at A-2; NSA DCLPO REPORT, *supra*, at 4; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

"target" of a traditional FISA electronic surveillance "is the individual or entity . . . about whom or from whom information is sought."[137]

There are technical reasons why "about" collection is necessary to acquire even some communications that are "to" and "from" a tasked selector. In addition, some types of "about" communications actually involve Internet activity of the targeted person.[138] The NSA cannot, however, distinguish in an automated fashion between "about" communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.[139]

In order to acquire "about" communications while complying with Section 702's prohibition on intentionally acquiring known domestic communications, the NSA is required to take additional technical steps that are not required for other Section 702 collection. NSA is required to use other technical means, such as Internet protocol ("IP") filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.[140] If, for example, a person located in Chicago sent an email to a friend in Miami that mentioned the tasked selector "JohnTarget@example.com," the IP filters (or comparable technical means) are designed to prevent the acquisition of this communication. The IP filters, however, do not operate perfectly,[141] and may fail to filter out a domestic communication before it is screened against tasked selectors. A United States-based user, for example, may send a communication (intentionally or otherwise) via a foreign server even if the intended recipient is also in the United States.[142] As such, the FISC has noted the government's concession that in the ordinary course of acquiring single communications, wholly domestic communications could be acquired as much as 0.197% of the time.[143] While this percentage is small, the FISA court estimated in 2011 that the

---

137 *See In re Sealed Case*, 310 F. 3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)); *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 55 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (confirming the FISC had held that targeting includes communications about a particular selector that are not necessarily to or from that selector).

138 Bates October 2011 Opinion, *supra*, at 37-38, 2011 WL 10945618, at *12 (describing the types of acquired Internet transactions and noting that a subset involve transactions of the target).

139 Bates October 2011 Opinion, *supra*, at 31, 43, 2011 WL 10945618, at *10, *14 (describing limitations on what can be distinguished at the acquisition stage).

140 Bates October 2011 Opinion, *supra*, at 33, 2011 WL 10945618, at *11 (regarding the "technical measures" that NSA uses to prevent the acquisition of upstream collection of domestic communications); NSA DCLPO REPORT, *supra*, at 5-6 (acknowledging that IP filters are used to prevent the acquisition of domestic communications).

141 December 2011 Joint Statement, *supra*, at 7 (acknowledging measures to prevent acquisition of domestic communications "are not perfect").

142 Bates October 2011 Opinion, *supra*, at 34-35 n.33, 2011 WL 10945618, at *11 n.33.

143 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

overall number of communications the government acquires through Section 702 upstream collection could result in the government acquiring as many as tens of thousands of wholly domestic communications per year.[144]

In addition, wholly domestic communications could also be acquired because they were embedded in a larger multi-communication transaction ("MCT"), the subject of the next section.

3. Upstream Collection of Internet Communications: Multi-Communication Transactions ("MCTs")

While the NSA's upstream collection is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*. The difference between *communications* and *transactions* is a significant one, and the government's failure to initially distinguish and account for this distinction caused the FISA court to misunderstand the nature of the collection for over two years, and later to find a portion of the Section 702 program to be unconstitutional.

The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet. An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet.[145] An Internet transaction could consist of a single discrete communication, such as an email that is sent from one server to another. Such communications are referred to as single communication transactions (SCTs).[146] Of the upstream Internet transactions that the NSA acquired in 2011, approximately ninety percent were SCTs.[147]

In other instances, however, a single Internet transaction might contain multiple discrete communications. These transactions are referred to as MCTs.[148] If a single discrete communication within an MCT is to, from, or about a Section 702–tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT.[149]

If the acquired MCT is a transaction between the Section 702 target (who is assessed to be a non-U.S. person located outside the United States and is targeted to acquire foreign intelligence information falling under one of the approved certifications) and a server, then

---

144 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32; December 2011 Joint Statement, *supra*, at 7.

145 *See* Bates October 2011 Opinion, *supra*, at 28 n.23, 2011 WL 10945618, at *9 n.23 (quoting government characterization of what constitutes an Internet transaction).

146 Bates October 2011 Opinion, *supra*, at 27-28, 2011 WL 10945618, at *9.

147 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

148 Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9.

149 December 2011 Joint Statement, *supra*, at 7.

all of the discrete communications acquired within the MCT are also communications to or from the target. Based on a statistical sample conducted by the NSA, the FISC estimated that as of 2011 the NSA acquired between 300,000 and 400,000 such MCTs every year (i.e., MCTs where the "active user,"[150] was the target him or herself).[151]

When the acquired MCT is not a transaction between the target and the server, but instead a transaction between another individual and a server that happens to include a Section 702 tasked selector, the MCT may "include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship to the [tasked] selector."[152] These non-target MCTs break down into three categories. Based on the NSA's statistical study, the FISC estimated that (as of 2011) the NSA acquired at least 1.3 million MCTs each year where the user who caused the transaction to occur was not the target, but was located outside the United States.[153] Using this same statistical analysis, the FISA court estimated that the NSA would annually acquire an additional approximately 7,000 to 8,000 MCTs of non-targeted users who were located in the United States, and between approximately 97,000 and 140,000 MCTs each year where NSA would not be able to determine whether the user who caused the transaction to occur was located inside or outside the United States.[154]

The NSA's acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector."[155] While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided.[156] If time

---

150 The "active user" is the actual human being who is interacting with a server to engage in an Internet transaction.

151 Bates October 2011 Opinion, *supra*, at 38, 2011 WL 10945618, at *12.

152 December 2011 Joint Statement, *supra*, at 7.

153 Bates October 2011 Opinion, *supra*, at 39, 2011 WL 10945618, at *12.

154 Bates October 2011 Opinion, *supra*, at 38-40, 2011 WL 10945618, at *12. With respect to this last category, the unidentified user could be the Section 702 target. *Id.* at 38, 40-41, 2011 WL 10945618, at *12.

155 Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *10. In 2011, the NSA was able to determine that approximately 90 percent of all upstream Internet transactions consisted of SCTs as the result of a post-acquisition statistical sample that required a manual review. *Id.* at 34 n.32, 2011 WL 10945618, at *11.

156 Bates October 2011 Opinion, *supra*, at 32, 2011 WL 10945618, at *10.

were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that filter would be out-of-date as soon as time was restarted and a protocol changed, a new service or function was offered, or a user changed his or her settings to interact with the Internet in a different way. Conducting upstream Internet acquisition will therefore continue to result in the acquisition of some communications that are unrelated to the intended targets.

The fact that the NSA acquires Internet communications through the acquisition of Internet transactions, be they SCTs or MCTs, has implications for the technical measures, such as IP filters, that the NSA employs to prevent the intentional acquisition of wholly domestic communications. With respect to SCTs, wholly domestic communications that are routed via a foreign server for any reason are susceptible to Section 702 acquisition if the SCT contains a Section 702 tasked selector.[157] With respect to MCTs, wholly domestic communications also may be embedded within Internet transactions that also contain foreign communications with a Section 702 target. The NSA's technical means for filtering domestic communications cannot currently discover and prevent the acquisition of such MCTs.[158]

Because of the greater likelihood that upstream collection of Internet transactions, in particular MCTs, will result in the acquisition of wholly domestic communications and extraneous U.S. person information, there are additional rules governing the querying, retention, and use of such upstream data in the NSA minimization procedures. These additional procedures are discussed below.

IV. Targeting Procedures: Who May Be Targeted? How? And Who Decides?

As is discussed above, the government targets persons under Section 702 by tasking selectors — communication facilities, such as email addresses and telephone numbers — that the government assesses will be used by those persons to communicate or receive foreign intelligence information that falls within one of the authorized Section 702 certifications.[159] Under Section 702, this targeting process to determine which persons are (1) non-U.S. persons, that are (2) reasonably believed to be located outside the United States, who will (3) use the tasked selectors to communicate or receive foreign intelligence

---

157 Bates October 2011 Opinion, *supra*, at 34-35, n.32 & n.33; *id*. at 45, 2011 WL 10945618, at *11 ("[T]he government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server.")

158 Bates October 2011 Opinion, *supra*, at 45, 47, 2011 WL 10945618, at *15.

159 *See, e.g.*, AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-2.

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

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
JULIA BERMAN
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-4373-JSW **CLASSIFIED DECLARATION OF MIRIAM P., NATIONAL SECURITY AGENCY *EX PARTE, IN CAMERA* SUBMISSION** Date: December 19, 2014 Time: 9:00 a.m. Courtroom 5, 2nd Floor The Honorable Jeffrey S. White

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

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

1. (U) I, Miriam P., do hereby state and declare as follows:

2. (U) I am the Deputy Chief of Staff for Signals Intelligence (SIGINT) Policy and Corporate Issues for the Signals Intelligence Directorate (SID) of the National Security Agency (NSA), an intelligence agency within the Department of Defense.

3. (U) I am responsible for, among other things, protecting NSA SIGINT activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, the NSA SIGINT Directorate is responsible for the collection, processing, and dissemination of SIGINT information for the foreign intelligence purposes of the United States. 46 Fed. Reg. 59941 (Dec. 4, 1981) as amended by Executive Order 13284 (2003). Executive Order 13355 (2004), 69 Fed. Reg. 53,593 (Aug. 27, 2004); Executive Order 13470 (2008), 73 Fed. Reg. 45325. I have been designated an original TOP SECRET classification authority under Executive Order (E.O.) 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb, 24, 2012).

4. (U) My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, the information available to me in my capacity as the Deputy Chief of Staff for SIGINT Policy and Corporate Issues for SID, and the advice of counsel.

5. (U) I submit this declaration for three purposes. First, this declaration describes on the public record, to the extent practicable, the effectiveness of the NSA's "Upstream" collection of communications under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") as a method of gathering foreign intelligence information. Second, this declaration provides some details on the effectiveness of the program that cannot be disclosed on the public record. Although the Government has released to the public some information about NSA's Upstream collection, the operational details and much of the information about its effectiveness, set forth below in classified paragraphs, has not been officially disclosed and remains classified. Because the disclosure of this information could reasonably be expected to cause exceptionally grave damage to national security, it falls within the NSA's claim of statutory privilege under Section 6

of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50 U.S.C. § 3601 *et seq.*), *see* Classified, *Ex Parte* Declaration of Frances J. Fleisch, NSA ¶¶ 8, 44(B)(1)(b) (Dec. 20, 2013), which, in turn, formed the basis of the assertion of the state secrets privilege by the Director of National Intelligence ("DNI"). *See* Public Declaration of James R. Clapper, DNI (Sept. 11, 2012) (ECF No. 104) ¶¶ 3, 9, 11; Public Declaration of James R. Clapper, DNI (Dec. 20, 2013) (ECF No. 168) ¶¶ 4, 9, 11, 19.C.1.b. And finally, I describe the impracticability of obtaining a warrant each time the NSA needs to target a selector for Upstream collection of communications.

6. (U) Under the authority of Section 702 of the FISA Amendments Act ("FAA") the NSA acquires information through two different methods. Under the PRISM collection, the government sends selectors, such as an e-mail address, to a United States-based electronic communication service provider that has been served with a directive issued in accordance with the criteria of Section 702. The provider, such as an Internet Service Provider ("ISP"), then furnishes to the government the communications from specific accounts that have been targeted for collection. The content of telephone calls is not acquired through the PRISM collection. I understand that PRISM collection is not at issue in the current motions practice before the Court.

7. (U) Upstream collection, in contrast, involves the compelled assistance (through a Section 702 directive) of certain providers that control the telecommunications backbone over which telephone and Internet-based communications transit. Unlike PRISM, Upstream collection generally involves the acquisition of certain communications as they traverse the telecommunications backbone.

(U) Impracticability of Acquiring the Same Information through Other Methods

8. (U) The NSA's Upstream collection is capable of acquiring certain types of targeted communications containing valuable foreign intelligence information that cannot be collected under PRISM or other SIGINT methods authorized by FISA.

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

9. ~~(TS//SI//NF)~~ [redacted]

10. ~~(TS//SI//NF)~~ [redacted]

11. ~~(TS//SI//NF)~~ [redacted]

12. (U) In addition, unlike 702 PRISM collection, 702 Upstream is a valuable source of "abouts" collection in which the targeted identifier (e.g., an e-mail address) is contained in the

content of the communication. For example, a communication would be acquired via Upstream collection if the targeted selector was found only in the body of an e-mail message and not in the "to/from" line.

13. (U) "Abouts" communications are a valuable source of foreign intelligence information that cannot be obtained through other FISA collection techniques currently used, including PRISM collection.

14. ~~(S//SI//NF)~~ [redacted]

15. ~~(TS//SI//NF)~~ [redacted]

16. (U) Acquiring the content of certain telephone calls through Upstream collection allows NSA to acquire significant foreign intelligence information that it may not otherwise obtain through other methods of signals intelligence.

[1] ~~(TS//SI//NF)~~ [redacted]

(U) Contribution of Upstream Collection to NSA's Mission

17. (U) Upstream collection fills a critical gap in U.S. intelligence gathering. Upstream collection has enabled the NSA to acquire—quickly and effectively—a greater range of foreign intelligence information that it otherwise would not be able to obtain. Upstream collection is a proven critical tool in the collection of significant and sometimes uniquely valuable foreign intelligence information necessary to protect the Nation's security. It allows the NSA to direct collection against targets quickly so that the NSA can nimbly turn collection into actionable intelligence leads for the Intelligence Community. Below is an outline of some of the ways Upstream collection has contributed significantly to the NSA's mission to defend the United States and its interests at home and abroad.

18. ~~(TS//SI//NF)~~ [redacted]

~~(TS//SI//NF)~~ [redacted]

19. ~~(TS//SI//NF)~~ [redacted]

20. ~~(TS//SI//NF)~~ [redacted]

[redacted]

21. ~~(TS//SI//NF)~~ [redacted]

[redacted]

22. ~~(TS//SI//NF)~~ [redacted]

[redacted]

23. ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

24. ~~(TS//SI//NF)~~ [redacted]

[redacted]

[2] ~~(TS//SI//NF)~~ [redacted]

25. ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

26. ~~(TS//SI//NF)~~ [redacted]

[redacted]

27. ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

28. ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

29. ~~(TS//SI//NF)~~ [redacted]

[redacted]

30. ~~(TS//SI//NF)~~ [redacted]

[redacted]

31. ~~(TS//SI//NF)~~ [redacted]

(U) Impracticality of Obtaining a Warrant

32. (U) The reasons for which the Government sought the authority and renewal of the authority provided in Section 702 to collect intelligence targeted at non-U.S. persons located outside the United States without individualized warrants apply to both of NSA's methods of collection under Section 702—Upstream and PRISM.

33. (U) Requiring the NSA to obtain a FISA (or other type of) warrant each time the NSA needs to target a selector tasked for Upstream collection would be impractical and could result in the loss of critical foreign intelligence information such as that described above. Requiring the Government to obtain a warrant each time the NSA needed to task a selector also would be impractical given the significant number of selectors that need to be tasked for Upstream collection. Additionally, given that the collection of signals intelligence to obtain foreign intelligence information requires speed and flexibility so that NSA can respond to new and quickly evolving threats facing our nation, imposing a warrant requirement would reduce the

NSA's flexibility and significantly slow its ability to respond to fast-moving threat scenarios and evolving efforts by our adversaries to evade detection through frequent shifts in their communication patterns or platforms. Such a warrant requirement would also impose an extraordinary burden on the NSA's intelligence resources, diverting resources from mission critical activities. And, finally, the delays inherent in such a requirement would impede the NSA's ability to collect critical and time-sensitive foreign intelligence information. Critical intelligence would be lost.

(U) Conclusion

34. (U) The information set forth in the classified paragraphs above fall within the NSA's assertion of statutory privilege under Section 6 of the National Security Agency Act, which, in turn, formed the basis of the DNI's assertion of the state secrets privilege and so cannot be disclosed for purposes of addressing the allegations in Plaintiffs' Combined Reply in Support of their Motion for Partial Summary Judgment and Opposition to the Government Defendants' Cross-Motion for Partial Summary Judgment (or for any other purpose) without risking exceptionally grave damage to national security.

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

DATE: November 7, 2014

Miriam P.

(U) Miriam P.
(U) Deputy Chief of Staff for
SIGINT Policy and Corporate Issues, Signals
Intelligence Directorate

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
BENJAMIN W. BERKOWITZ (SBN 244441)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700
Fax: (650) 813-9777

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **OCTOBER 24, 2014 DECLARATION OF RICHARD R. WIEBE IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT** **(Fourth Amendment Violation)** Date: December 19, 2014 Time: 9:00 a.m. Courtroom 5, Second Floor The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. Except as otherwise stated below, I could and would testify competently to the following.

2. **Exhibit A:** Attached hereto as Exhibit A is a true and correct copy of pages 33-34 of the Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("PCLOB 702 Report"), *available at* http://www.pclob.gov/All Documents/Report on the Section 702 Program/PCLOB-Section-702-Report.pdf.

3. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of AT&T Inc.'s transparency report for the first half of 2014, *available at* http://about.att.com/content/dam/csr/PDFs/ATT_Transparency%20Report_July%202014.pdf.

4. **Exhibit C:** Attached hereto as Exhibit C is a true and correct copy of an excerpt from the court reporter's transcript of the hearing held June 24, 2006 in the United States District Court for the Northern District of California before Chief District Judge Vaughn R. Walker in the related action of *Hepting v. AT&T*, No. 06-CV-0672-VRW.

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

Executed at San Francisco, CA on October 24, 2014.

s/ *Richard R. Wiebe*
Richard R. Wiebe

EXHIBIT A

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

considered targets — and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process.

Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden").[114] Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.[115]

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.[116]

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or "ISP") that has been served a directive.[117] Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only "about" the selector, as described below).[118] As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), a*vailable at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company "would have received legal process").

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.[119]

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company ("USA-ISP Company") may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address "johntarget@usa-ISP.com" to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.[120] The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.[121]

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

---

119 Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

120 Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 6(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

121 NSA 2011 Minimization Procedures, *supra*, § 6(c).

EXHIBIT B

AT&T
Transparency Report

Introduction

We take our responsibility to protect your information and privacy very seriously. We continue our pledge to protect your privacy to the fullest extent possible and in compliance with the laws of the country where your service is provided.

Like all companies, we are required by law to provide information to government and law enforcement agencies, as well as parties to civil lawsuits, by complying with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid, and that our responses comply with the law and our own policies.

This Report

AT&T's first Transparency Report provided information for 2013. In fulfillment of our commitment to issue reports on a semiannual basis, this report provides specific information regarding the number and types of demands to which we responded from Jan. 1, 2014 through June 30, 2014, as well as National Security Demands for the second half of 2013 which we are providing subject to the U.S. Department of Justice's guidelines. This report doesn't include any numbers or information for Cricket™ Wireless because they weren't acquired until March 2014. We plan to include Cricket's data in our next report.

What's New?

We appreciate the comments we received on AT&T's first Transparency Report. We have incorporated changes to provide you with more transparency. These changes include:

- Disclosing the specific number of wiretaps, pen registers, and general court orders processed.
- A clearer statement that we require a search warrant or probable cause order before providing any stored content.

The chart below includes hyperlinks to additional information on the category of data reported.

NATIONAL SECURITY DEMANDS

National Security Letters (Jan. 1 – June 30, 2014)	
▪ Total Received	1,000-1,999
▪ Number of Customer Accounts	2,000-2,999
Foreign Intelligence Surveillance Act (July 1 – Dec. 31, 2013) [1]	
▪ Total Content	0-999
○ Customer Accounts	33,000-33,999
▪ Total Non-Content	0-999
○ Customer Accounts	0-999

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

Total Demands (Federal, State and Local; Criminal and Civil)			**115,925**
▪ Subpoenas		**86,943**	
○ Criminal	78,975		
○ Civil	7,968		
▪ Court Orders (General)		**15,105**	
○ Historic	12,569		
○ Real-time (Pen registers)	2,536	**9,393**	
▪ Search Warrants/Probable Cause Court Orders			
○ Historic			
▪ Stored Content	2,532		
▪ All Others	6,861		
○ Real-Time		**4,484**	
▪ Wiretaps	1,167		
▪ Mobile Locate Demands	3,317		

[1] The Department of Justice imposes a six-month delay for reporting this data.

DEMANDS REJECTED/PARTIAL OR NO DATA PROVIDED (Breakout detail of data included in Total U.S. Criminal & Civil Litigation)		
Total		**31,097**
▪ Rejected/Challenged	2,110	
▪ Partial or No Information	28,987	

LOCATION DEMANDS (Breakout detail of data included in Total U.S. Criminal & Civil Litigation)		
Total		**30,886**
▪ Historical	23,646	
▪ Real-time	6,956	
▪ Cell Tower Searches	284	

EMERGENCY REQUESTS		
Total		**50,232**
▪ 911	39,449	
▪ Exigent	10,783	

INTERNATIONAL DEMANDS		
Total Demands		**17**
▪ Law Enforcement	11	
▪ URL/IP Blocking	6	

Explanatory Notes

NATIONAL SECURITY DEMANDS

The Department of Justice's guidance, issued on Jan. 27, 2014, authorized us to report on the receipt of National Security Letters and court orders issued under the Foreign Intelligence Surveillance Act (FISA), with the exception of data, if any, related to the so-called bulk telephony metadata program. *See* http://www.justice.gov/opa/pr/2014/January/14-ag-081.html.

National Security Letters are subpoenas issued by the Federal Bureau of Investigation in regard to counterterrorism or counterintelligence. These subpoenas are limited to non-content information, such as a list of phone numbers dialed or subscriber information.

Court orders issued pursuant to FISA may direct us to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage.

These types of demands have very strict policies governing our ability to disclose the requests. The recent "Statistical Transparency Report Regarding Use of National Security Authorities" published by the Director of National Intelligence on June 26, 2014, does not alter the Department of Justice's Jan. 27, 2014, guidance.
See http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013.

Consistent with guidance from January 2014, our report includes the range of customer accounts potentially impacted by these National Security Demands.

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

This number includes demands to which we responded in connection with criminal and civil litigation matters. This category doesn't include demands reported in our National Security Demands table.

Criminal proceedings include actions by the government — federal, state, and local — against an individual arising from an alleged violation of applicable criminal law.

Civil actions include lawsuits involving private parties (i.e., a personal liability case, divorce proceeding, or any type of dispute between private companies or individuals). In addition, civil proceedings include investigations by governmental regulatory agencies such as the Securities and Exchange Commission, the Federal Trade Commission and the Federal Communications Commission.

We ensure we receive the right type of legal demand.

We receive several types of legal demands, including subpoenas, court orders, and search warrants. Before we respond to **any** legal demand, we determine that we have received the correct type of demand based on the applicable federal and state laws and the type of information being sought. For instance, in some states we must supply call detail records if we receive a subpoena. In other states, call detail records require a court order or search warrant. If the requesting agent has failed to send the correct type of demand, we reject the demand.

Types of Legal Demands

Subpoenas, court orders and search warrants are used to demand information for use in criminal trials, lawsuits, investigations, and other proceedings. If the applicable rules are followed, we're legally required to provide the information.

In this, our second report, we have changed the reporting for "Total U.S. Criminal & Civil Demands" to more accurately reflect the type of demand with the information requested, particularly relating to general court orders and search warrants.

- **Subpoenas** don't usually require the approval of a judge and are issued by an officer of the court. They are used in both criminal and civil cases, typically to obtain written business documents such as calling records.

- **General Court Orders** are signed by a judge. We consider "general" court orders as all orders except those that contain a probable cause finding. In a criminal case, for example, a judge may issue a court order on a lesser standard than probable cause, such as "relevant to an ongoing criminal investigation." In a civil case, a court order may be issued on a "relevant" or "reasonably calculated to lead to the discovery of admissible evidence" standard. For this report, general court orders were used to obtain historical information like billing records or the past location of a wireless device. In criminal cases, they are also used to obtain real-time, pen register/"trap and trace" information, which provides phone numbers and other dialed information for all calls as they are made or received from the device identified in the order.

- **Search Warrants and Probable Cause Court Orders** are signed by a judge, and they are issued only upon a finding of "probable cause." To be issued, the warrant or order must be supported by sworn testimony and sufficient evidence to believe the information requested is evidence of a crime. Probable cause is viewed as the highest standard to obtain evidence. Except in emergency circumstances, a search warrant or probable cause court order for all real-time location information (i.e., wiretaps and GPS) and stored

content (i.e., text and voice messages) is required for all jurisdictions, courts, and agencies.

DEMANDS REJECTED/PARTIAL OR NO DATA PROVIDED

We ensure that we receive the appropriate type of demand for the information requested. In this category, we include the number of times we rejected a demand or provided only partial information or no information in response to a demand. Here are a few reasons why certain demands fall into this category:

- The wrong type of demand is submitted by law enforcement. For instance, we will reject a subpoena requesting a wiretap, because either a probable cause court order or search warrant is required.
- The demand has errors, such as missing pages or signatures.
- The demand was not correctly addressed to AT&T.
- The demand did not contain all of the elements necessary for a response.
- We had no information that matched the customer or equipment information provided in the demand.

LOCATION DEMANDS

Our Location Demands category breaks out the number of court orders and search warrants we received by the type of location information (historical and real-time) they requested. We also provide the number of requests we received for cell tower searches, which ask us to provide all telephone numbers registered to a particular cell tower for a certain period of time (or to confirm whether a particular telephone number registered on a particular cell tower at a given time). We do not keep track of the number of telephone numbers provided to law enforcement in connection with cell tower searches.

A single cell tower demand may cover multiple towers. In our last report, we disclosed the total number of cell tower searches. For clarity, we are now disclosing the total numbers of demands and the total number of searches. For instance, if we received one court order that included ID numbers for two cell towers, we count that as one demand for two searches. For the 284 cell tower demands during this period, we performed 708 searches. We also maintain a record of the average time period that law enforcement requests for one cell tower search, which was 2 hours, 23 minutes for this reporting period.

Except in emergency situations, we require the most stringent legal standard — a search warrant or probable cause court order — for all demands for specific location information. The legal standard required for the production of other location data is unsettled. Some courts have

decided that a general court order is sufficient legal process for law enforcement to obtain such location data. Other courts have determined that the Fourth Amendment requires law enforcement to first obtain a search warrant or probable cause court order before seeking this location information. With the exception of emergency situations, we require an order signed by a judge before producing any type of location information to law enforcement. We will continue to follow these legal developments and, in all circumstances, we will comply with the applicable law.

EMERGENCY REQUESTS

This category includes the number of times we responded to 911-related inquiries and "exigent requests" to help locate or identify a 911 caller. These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. The numbers provided in this category are the total of 911 and exigent searches that we processed during this reporting period.

Even when responding to an emergency, we protect your privacy:

- When responding to 911 inquiries, we confirm the request is coming from a legitimate Public Safety Answering Point before quickly responding.
- For exigent requests, we receive a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we share information.

INTERNATIONAL DEMANDS

International Demands represent the number of demands we received from governments outside the U.S., and relate to AT&T's global business operations in these countries. Such International Demands are for customer information stored in their countries, and URL/IP (website/Internet address) blocking requests.

We are not a content provider outside the U.S. but are required by some countries' laws to comply with requests to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate in certain countries. These requests might be designed to block sites related to displaying child pornography, unregistered and illegal gambling, defamation, illegal sale of medicinal products, or trademark and copyright infringement. A demand may request that one or more identifiers (i.e., IP addresses or URLs) be blocked.

The majority of law enforcement demands involve requests for information relating to individuals. Because our global operations support only very large multi-national business customers, we received relatively few international demands. We do not have a mobility network outside the U.S., and we don't provide services to individual consumers residing outside the U.S. We received no demands from the U.S. government for data stored outside the U.S. If we receive an international demand for information stored in the U.S., we refer it to that country's Mutual Legal Assistance Treaty (MLAT) process. The Federal Bureau of Investigation ensures that we receive the proper form of U.S. process (e.g., subpoena, court order or search warrant), subject to the

limitations placed on discovery in the U.S., and that cross-border data flows are handled appropriately. Thus, any international-originated demands that follow an MLAT procedure are reported in our Total Demands category because we can't separate them from any other Federal Bureau of Investigation demand we may receive.

ADDITIONAL RESOURCES

You'll find more on our commitment to privacy in:

- Our Privacy Policy.
- Our issues brief on Privacy.
- Our issues brief on Freedom of Expression.

EXHIBIT C

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE VAUGHN R. WALKER, JUDGE

TASH HEPTING, et al.,

Plaintiffs,

v. 06 C 0672 VRW

AT&T Corp., et al.,

Defendants.

San Francisco, CA
June 23, 2006
9:40 a.m.

Pages 1 - 121

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

HELLER, EHRMAN, LLP
Attorneys for Plaintiffs
BY: ROBERT D. FRAM
NATHAN E. SHAFROTH
ELENA DiMUZIO

ELECTRONIC FRONTIER FOUNDATION
Attorneys for Plaintiffs
BY: CINDY COHN
KEVIN S. BANKSTON
KURT OPSAHL
LEE TIEN

LERACH, COUGHLIN, STOIA, GELLER,
RUDMAN & ROBBINS, LLP
Attorneys for Plaintiffs
BY: JEFF D. FRIEDMAN
MARIA V. MORRIS
REED R. KATHREIN

RICHARD R. WIEBE
Attorney for Plaintiffs

CONNIE KUHL, RMR, CRR
Official Reporter - U.S. District Court (415) 431-2020

APPEARANCES (cont.):

THE UNITED STATES OF AMERICA, DOJ
The Office of the Attorney General
BY: PETER D. KEISLER, Assistant Attorney General
CARL J. NICHOLS, Deputy Assistant Attorney General
JOSEPH HUNT

PILLSBURY, WINTHROP, SHAW & PITTMAN, LLP
Attorneys for Defendants AT&T Corp., et al.
BY: BRUCE A. ERICSON
DAVID L. ANDERSON
JACOB R. SORENSEN

SIDLEY, AUSTIN, LLP
Attorneys for Defendants AT&T Corp., et al.
BY: BRADFORD A. BERENSON

LEVY, RAM & OLSON, LLP
Attorneys for Intervenors The San Francisco Chronicle, LA Times, San Jose Mercury News, Bloomberg News, Associated Press
BY: KARL OLSON

QUINN EMANUEL
Attorneys for Intervenors Lycos and Wired News
BY: TIMOTHY L. ALGER

Reported By: Connie Kuhl, RMR, CRR
Official Court Reporter

Friday, June 23rd, 2006

9:40 a.m.

DEPUTY CLERK: Calling civil Case 06-0672, Tash Hepting, et al. versus AT&T Corporation, et al.

Counsel, state your appearances, please.

MR. FRAM: Robert Fram, Heller, Ehrman, for the plaintiffs, your Honor.

THE COURT: Good morning.

MR. BANKSTON: Kevin S. Bankston, Electronic Frontier Foundation for the plaintiffs, your Honor.

THE COURT: Good morning, sir.

MS. COHN: Cindy Cohn, Electronic Frontier Foundation, for the plaintiffs, your Honor.

THE COURT: Miss Cohn, good morning.

MR. TYRE: James Tyre, also for plaintiffs.

THE COURT: Good morning, Mr. Tyre.

MR. WIEBE: Richard Wiebe for the plaintiffs.

MR. OPSAHL: Kurt Opsahl, also for the plaintiffs.

MR. TIEN: Lee Tien for the plaintiffs.

MR. FRIEDMAN: Jeff Friedman, Lerach, Coughlin, for the plaintiffs.

THE COURT: Is that it?

MR. BERENSON: Bruce Berenson from Sidley, Austin, for Defendants AT&T.

THE COURT: Good morning.

one and two. I don't know if you want that now or reserve that --

THE COURT: Why don't we use that in any wrap-up we have, any wrap-up discussion. All right?

MR. FRAM: Thank you, your Honor.

THE COURT: Thank you, Mr. Fram.

Very quickly, Mr. Keisler? It is Keisler?

MR. KEISLER: It is, your Honor.

First of all, with respect to the suggestion that the plaintiffs already put forward a prima facie case. They note correctly that we haven't said any documents are classified. They say we can't now unring that bell. We don't want to unring that bell. None of the documents they have submitted to accompany these declarations implicate any privileged matters.

THE COURT: Including the Klein documents.

MR. KEISLER: We have not asserted any privilege over the information that is in the Klein and Marcus declarations.

THE COURT: Either in the declaration or its exhibits?

MR. KEISLER: We have not asserted a privilege over either of those. Mr. Klein and Marcus never had access to any of the relevant classified information here, and with all respect to them, through no fault or failure of their own, they don't know anything. And that's clear from the face of the declarations. And since Mr. Fram talked about them some, I may respond on that.

The plaintiffs rely on Mr. Klein's declaration of the asserted connection between AT&T and the NSA. Absolutely every assertion he makes in his declaration about that relationship is hearsay. It's one person told me that a third person who briefly visited the AT&T offices was from the NSA. And the statement that Mr. Fram quoted --

THE COURT: It has to be admissible in the summary judgment stage; we're not there yet.

MR. KEISLER: I'm just addressing whether they have a prima facie case, which I understand would be a case if the Court could issue a judgment, if it were unrebutted.

THE COURT: The absence of a rebuttal.

MR. KEISLER: And saying to my knowledge no one was permitted in a particular AT&T room who was not cleared by the NSA without giving any basis, not even a hearsay basis, for that claim of knowledge, would not be an element even of a prima facie case.

And with respect to Mr. Marcus, he acknowledges that he doesn't actually know even what equipment is in any room at AT&T. He's reading from a document, and all he testifies to as to what he understands are the capabilities of that equipment to be, and he says those capabilities are consistent with what he's read in the newspapers. But he doesn't know whether those pieces of equipment, if they're there, are actually used for those capabilities. And he acknowledges that that equipment

also has what he calls other legitimate possible uses. So the notion that this mixture of hearsay and speculation could be a prima facie case sufficient to sustain a judgment in the absence of rebuttal we think is just wrong.

But even if they had a more robust case, even if they had a real prima facie case, your Honor would run exactly into the portion of *Kasza* which your Honor quoted which is that even if plaintiffs can bring forward some non privileged evidence, if the very subject of the action is a state secret or if state secrets would prevent the defendant from producing important information in its defense, then judgment can be entered.

THE COURT: Isn't this case different, though? Different from the *Kasza* case? After all, *Kasza* dealt with a situation in which the whole program of disposing of these materials at the Grooms Lake facility or wherever it was, was involved and could not litigate the case without getting into that entire program disposal, and indeed it was the program of disposal that was the state secret. So the state secret was coextensive with all the evidence necessary for a plaintiff to proceed in that case, and it's not our case here, is it.

MR. KEISLER: We think it's exactly the case. The *Kasza* case said, no procedures can be at suit because classified information is an essential element of every one of the claims. We think that is precisely the case here.

Obviously they can't prove liability against AT&T

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

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
JULIA BERMAN
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.* Plaintiffs. v. NATIONAL SECURITY AGENCY, *et al.* Defendants.	Case No. 4:08-cv-4373-JSW **CLASSIFIED DECLARATION OF MIRIAM P., NATIONAL SECURITY AGENCY EX PARTE, IN CAMERA SUBMISSION** Date: October 31, 2014 and November 3, 2014 Time: 9:00 a.m. Courtroom 5, 2nd Floor The Honorable Jeffrey S. White

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

~~Classified By: NSA~~
~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20070108~~
~~Declassify On: 20641001~~

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

1. (U) I, Miriam P., do hereby state and declare as follows:

2. (U) I am the Deputy Chief of Staff for Signals Intelligence (SIGINT) Policy and Corporate Issues for the Signals Intelligence Directorate (SID) of the National Security Agency (NSA), an intelligence agency within the Department of Defense.

3. (U) I am responsible for, among other things, protecting NSA SIGINT activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, the NSA SIGINT Directorate (SID) is responsible for the collection, processing, and dissemination of SIGINT information for the foreign intelligence purposes of the United States. 46 Fed. Reg. 59941 (Dec. 4, 1981) as amended by Executive Order 13284 (2003). Executive Order 13355 (2004), 69 Fed. Reg. 53,593 (Aug. 27, 2004); Executive Order 13470 (2008), 73 Fed. Reg. 45325. I have been designated an original TOP SECRET classification authority under Executive Order (E.O.) 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb. 24, 2012).

4. (U) My statements herein are based upon my personal knowledge of SIGINT collection and NSA operations, the information available to me in my capacity as the Deputy Chief of Staff for SID for SIGINT Policy and Corporate Issues, and the advice of counsel.

5. (U) I submit this declaration to advise the Court of particular operational details of the NSA's "Upstream" collection of communications under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") that are implicated by Plaintiffs' Motion for Partial Summary Judgment (ECF No. 261) ("Plaintiffs' motion"). Although the Government has released to the public some information about NSA's Upstream collection, the operational details discussed herein have not been officially disclosed and remain classified. Because disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security, it falls within the December 20, 2013, claim of the state secrets privilege made by the Director of National Intelligence ("DNI") in this case, as well as NSA's claim of statutory

privilege under Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50 U.S.C. 3601 *et seq.*). *See* Classified, *In Camera, Ex Parte* Declaration of Frances J. Fleisch, NSA ¶¶ 8, 44(B)(1)(b) (Dec. 20, 2013) ("Fleisch Decl.").

6. ~~(TS//SI//NF)~~ [redacted]

7. ~~(TS//SI//NF)~~ I have reviewed the description in Plaintiffs' motion of the Upstream collection process. [redacted]

8. (U) First, Upstream collection under Section 702 is limited to the acquisition of communications, to, from, or about tasked selectors reasonably believed to be located outside the United States to acquire foreign intelligence information.

9. ~~(TS//SI//NF)~~ [redacted]

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

[redacted]

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

[redacted]

[redacted]

[redacted]

16. ~~(TS//SI//NF)~~ The above operational details concerning the Upstream collection process, if disclosed, would provide our Nation's adversaries [redacted]

[redacted]

[redacted] with unparalleled insight into exactly how the Upstream process works, and [redacted] to further refine and advance their capabilities to avoid NSA surveillance. [redacted]

17. (U) Therefore, this information falls within the scope of the DNI's assertion of the state secrets privilege, and the NSA's assertion of statutory privilege under Section 6 of the National Security Agency Act, and cannot be disclosed for purposes of addressing the allegations in Plaintiffs' partial motion for summary judgment (or any other purpose) without risking exceptionally grave damage to national security.

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

DATE: 9/29/2014

Miriam P.

(U) Miriam P.

EXHIBIT C

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

For now, therefore, "about" collection is an inextricable part of the NSA's upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether "about" collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by "about" collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of "about" communications — so that a debate can be had in which the national security benefits of the different forms of "about" collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of "about" collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what "about" collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding "about" collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of "about" collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, "about" communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions ("MCTs")

The technical means used to conduct the NSA's upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet "backbone," the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or "about" a tasked selector) in the process of acquiring a communication that *is* authorized for collection (because it is to, from, or "about" a tasked selector). In 2011, the FISA court held that the NSA's procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA's collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board's assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415/436-9333; Fax: 415/436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

DECLARATION OF JOICE WALTON IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

Date: October 31, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Joice Walton, hereby declare:

1. I am a plaintiff in this action, and I reside in San Jose, California. I am a high technology purchasing agent. I am also a music recording artist. The facts contained in the following affidavit are known to me of my own personal knowledge and if called upon to testify, I could and would competently do so.

2. I currently receive Internet access at my home through a subscription to AT&T's High Speed Internet DSL ("AT&T DSL") service. I have been a subscriber and user of this service since approximately February 2009.

3. Previously I was a subscriber and user of AT&T's Worldnet dial-up Internet ("AT&T Worldnet") service from at least October 2003 until February 2009.

4. I use the AT&T DSL service nearly every day. My most frequent uses of the Internet are email and browsing the Web. My previous use of the AT&T Worldnet service was very similar and just as frequent.

5. I have several email addresses included as part of my AT&T DSL service subscription (originally provided as part of my AT&T Worldnet subscription), which are hosted under the domain "att.net." The underlying service for these email addresses is provided by Yahoo! Inc.

6. I have relied on the AT&T DSL and Worldnet services to use the Internet to send and receive private messages of both a personal and professional nature. I have also accessed and sent other confidential and personal information via the Internet. I have always expected these activities to remain private.

7. My use of the Internet is particularly important to my career as a recording artist. I often promote my music to booking agents, promoters and fans, in person and online. I maintain a website at www.joicewalton.com, and I correspond with many of these individuals by email.

8. Some of the people I regularly correspond with about my music and about personal matters are located in foreign countries, including individuals located in Taiwan, Canada, France, Germany, the United Kingdom, and Spain. These correspondences have occurred throughout my time as an AT&T DSL and Worldnet subscriber and many of them continue up to the present. In

addition, from approximately 2004 to 2006, I corresponded on a near-daily basis with an individual in Saudi Arabia.

9. I occasionally visit websites hosted in foreign countries, but I feel that naming these websites would violate my privacy.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on July 17, 2014 at San Jose, California.

JOICE WALTON

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415/436-9333; Fax: 415/436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

DECLARATION OF ERIK KNUTZEN IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

Date: October 31, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Erik Knutzen, hereby declare:

1. I am a plaintiff in this action, and I reside in Los Angeles, California. I am a writer and author. The facts contained in the following affidavit are known to me of my own personal knowledge and if called upon to testify, I could and would competently do so.

2. I currently receive Internet access at my home through a subscription to AT&T's High Speed Internet DSL ("AT&T DSL") service. I have been a subscriber and user of this service since approximately May 2005.

3. Previously I was a subscriber and user of AT&T's Worldnet dial-up Internet ("AT&T Worldnet") service from at least October 2003 until May 2005.

4. I use the AT&T DSL service on a daily basis. I routinely use this service for email, to browse the web, and to access social media services including Facebook and Twitter. During my time as an AT&T Worldnet subscriber, I also used the service very frequently, primarily for email and web browsing.

5. I use several email addresses included as part of my AT&T DSL service subscription (originally provided as part of my AT&T Worldnet subscription), which are hosted under the domain "sbcglobal.net." The underlying service for these email addresses is provided by Yahoo! Inc.

6. I use the Internet to send private messages and correspondence and to conduct other private activities online. I expect my use of the AT&T DSL service (and my prior use of the AT&T Worldnet service) for these private activities to remain private.

7. Since approximately 2006, I have published a blog and recorded a podcast about urban homesteading and related issues. As part of these activities I have often corresponded with readers and listeners.

8. Some of these readers and listeners are in foreign countries. Throughout my time as an AT&T DSL and Worldnet subscriber and continuing up to the present, I have regularly exchanged private messages with individuals in many countries, including New Zealand, Holland, Denmark, and South Africa. A consultation of my email records shows that many of the

individuals in foreign countries with whom I correspond use email providers whose domains identify them as foreign.

9. I have also visited and read the websites of foreign press outlets and blogs on a regular basis, including the *Guardian* and the BBC.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on July 18, 2014 at Los Angeles, California.

ERIK KNUTZEN

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415/436-9333; Fax: 415/436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

DECLARATION OF CAROLYN JEWEL IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT

Date: October 31, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Carolyn Jewel, hereby declare:

1. I am a plaintiff in this action, and I reside in Petaluma, California. I am a database administrator. I am also a published author of fiction. The facts contained in the following affidavit are known to me of my own personal knowledge and if called upon to testify, I could and would competently do so.

2. I currently receive Internet access at my home through a subscription to AT&T's Mobile Share Value Plan 4G ("AT&T 4G") service. I have been a subscriber and user of this service since approximately February 2014.

3. Previously I was a subscriber and user of AT&T's Worldnet dial-up Internet ("AT&T Worldnet") service from approximately June 2000 until approximately 2011. Between 2011 and approximately February 2014, I subscribed to a number of Internet service providers, none of them affiliated with AT&T.

4. I use the AT&T 4G service nearly every day, to send and receive email, for web browsing, and to access social media services including Facebook and Twitter. I previously used my AT&T Worldnet subscription for the same purposes and with similar frequency.

5. I use the AT&T 4G service (and previously used the AT&T Worldnet service) to send correspondence and engage in activities that I expect to remain private, such as personal correspondence, banking, family matters, medical matters of concern to me, and discussions regarding my published and in-progress writing with my literary agent, editors, other members of the publishing industry, and other authors and fans.

6. Throughout my time as a subscriber to AT&T's Worldnet and 4G services and continuing up to the present, I have engaged in e-mail correspondence with individuals in many foreign countries, including England, Germany, Indonesia, New Zealand, and Australia. I regularly receive and respond to emails from fans, translators and others in foreign countries. A consultation of my email records shows that many of the individuals in foreign countries with whom I correspond use email providers whose domains identify them as foreign.

7. I have also regularly accessed websites that are hosted in foreign countries. Because many of my novels are set in the historical past, I often research factual material online that is

hosted by foreign sites. For example, I published a novel in 2009 called *Indiscreet*, which was set in Turkey and Syria, for which I did significant research on foreign websites about those countries. For other novels, I regularly visit the websites of libraries in the United Kingdom and elsewhere in order to access digitized content from those libraries.

8. I have also visited and read the websites of foreign press outlets, including the *Scotsman* and the BBC, as well as foreign archeology blogs, on a near-daily basis.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on July 15, 2014 at Petaluma, California.

CAROLYN JEWEL

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

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

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

JULY 25, 2014 DECLARATION OF RICHARD R. WIEBE IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

(Fourth Amendment Violation)

Date: October 31, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. Except as otherwise stated below, I could and would testify competently to the following.

2. Each exhibit attached hereto is a true and correct copy of the document located at the indicated source.

3. **Exhibit A:** Attached hereto as Exhibit A is a true and correct copy of pages 7, 24-25, 27, 35-37, 111, 121-22, and 137-38 of the Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("PCLOB 702 Report"), *available at* http://www.pclob.gov/All Documents/Report on the Section 702 Program/PCLOB-Section-702-Report.pdf.

4. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of NSA PRISM slides, published by the Guardian on November 1, 2013, *available at* http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document and also *available at* http://s3.documentcloud.org/documents/813847/prism.pdf.

5. **Exhibit C:** Attached hereto as Exhibit C is an excerpt from the NSA's Special Source Operations Weekly, March 14, 2013 edition, published by the Washington Post on October 30, 2013 *available at* http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/ and also *available at* http://s3.documentcloud.org/documents/813020/sso-weekly-excerpt-for-posting-redacted.pdf.

6. **Exhibit D:** Attached hereto as Exhibit D is a true and correct copy of pages 6-8 of the December 8, 2011 Joint Statement of Assistant Attorney General Lisa Monaco, National Security Agency Deputy Director John Inglis, and General Counsel, Office of the Director of National Intelligence, Robert Litt, *available at* http://www.dni.gov/files/documents/Joint Statement FAA Reauthorization Hearing - December 2011.pdf.

7. **Exhibit E:** Attached hereto as Exhibit E is a true and correct copy of figure 9, page 29 of Federal Communications Commission, Common Carrier Bureau, 1999 International

Telecommunications Data (Dec. 2000), *available at*: http://transition.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/Intl/4361-f99.pdf.

8. **Exhibit F:** Attached hereto as Exhibit F is a true and correct copy of page 183 of the President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

9. **Exhibit G:** Attached hereto as Exhibit G is a true and correct copy of pages 35-37 of the Testimony of the Hon. James Robertson (U.S. District Judge, ret.), "Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act" (July 9, 2013), *available at* http://www.pclob.gov/All Documents/July 9, 2013 Workshop Transcript.pdf.

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

Executed at San Francisco, California on July 25, 2014.

s/ *Richard R. Wiebe*
Richard R. Wiebe

EXHIBIT A

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.

Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or "tasks" certain "selectors," such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection.

In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The National Security Agency ("NSA") receives all data collected through PRISM. In addition, the Central Intelligence Agency ("CIA") and the Federal Bureau of Investigation ("FBI") each receive a select portion of PRISM collection.

Upstream collection differs from PRISM collection in several respects. First, the acquisition occurs with the compelled assistance of providers that control the telecommunications "backbone" over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies. Upstream collection also includes telephone calls in addition to Internet communications. Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data. Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called "about" communications and the acquisition of so-called "multiple communications transactions" ("MCTs"). An "about" communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being "to" or "from" the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be "about" the selector. An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or "about" a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency's use,

of the acquisition to be located in the United States."[63] Finally, Section 702 contains a limitation (and a reminder) that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment to the Constitution.[64]

B. Section 702 Certifications

The Attorney General and the Director of National Intelligence authorize Section 702 targeting in a manner substantially different than traditional electronic surveillance under FISA. To authorize traditional FISA electronic surveillance, an application approved by the Attorney General must be made to the FISC.[65] This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance; facts justifying a probable cause finding that this target is a foreign power or agent of a foreign power and uses (or is about to use) the communication facilities or places at which electronic surveillance is being directed;[66] minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance; and a certification regarding the foreign intelligence information sought.[67] If the FISC judge who reviews the government's application determines that it meets the required elements — including that there is probable cause that the specified target is a foreign power or agent of a foreign power and that the minimization procedures meet the statutory requirements — the judge will issue an order authorizing the requested electronic surveillance.[68]

Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualized determinations by the FISC. Under the statute, the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.[69] Instead of identifying particular individuals to be targeted under Section 702, the certifications identify categories of foreign intelligence information regarding which the Attorney

---

63 50 U.S.C. § 1881a(b)(4).

64 50 U.S.C. § 1881a(b)(5).

65 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. 50 U.S.C. § 1805(e).

66 *But see* 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders "in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown")

67 50 U.S.C. §§ 1804(a), 1805(a).

68 50 U.S.C. § 1805(a), (c), (d).

69 50 U.S.C. § 1881a(a); NSA DCLPO REPORT, *supra*, at 2 (noting that Section 702 certifications do not require "individualized determination" by the FISC).

General and Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad.[70] There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or agent of a foreign power, as is required under traditional FISA. Rather, the categories of information being sought must meet the definition of foreign intelligence information described above. The government has not declassified the full scope of the certifications that have been authorized, but officials have stated that these certifications have authorized the acquisition of information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.[71]

While individual targets are not specified, Section 702 certifications must instead contain "targeting procedures" approved by the Attorney General that must be "reasonably designed" to ensure that any Section 702 acquisition is "limited to targeting persons reasonably believed to be located outside the United States" and prevents the "intentional acquisition" of wholly domestic communications.[72] The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to possess or receive) the types of foreign intelligence information authorized by a certification. The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. In addition, the Attorney General and Director of National Intelligence must also attest in the certification that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program.[73] Most critically, these Attorney General Guidelines explain how the government implements the statutory prohibition against reverse targeting.

While only non-U.S. persons may be intentionally targeted, the information of or concerning U.S. persons may be acquired through Section 702 targeting in a variety of ways, such as when a U.S. person is in communication with a non-U.S. person Section 702

---

70 *See* 50 U.S.C. § 1881a(g)(2)(A)(v) (requiring Attorney General and Director of National Intelligence to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information); PCLOB March 2014 Hearing Transcript, *supra*, at 8-9 (statement of Robert Litt, General Counsel, ODNI) (stating that certifications "identify categories of information that may be acquired"); NSA DCLPO REPORT, *supra*, at 2 (noting the "annual topical certifications" authorized by Section 702).

71 PCLOB March 2014 Hearing Transcript at 13 (statement of Robert Litt, General Counsel, ODNI) (stating that the Section 702 program has been an important source of information "not only about terrorism, but about a wide variety of other threats to our nation"); *id*. at 59 (statement of Rajesh De, General Counsel, NSA) (stating that there are certifications on "counterterrorism" and "weapons of mass destruction"); *id*. at 68 (statement of James A. Baker, General Counsel, FBI) ("[T]his program is not limited just to counterterrorism.").

72 50 U.S.C. § 1881a(d)(1), (g)(2)(A)(i), (g)(2)(B).

73 50 U.S.C. § 1881a(f), (g)(2)(A)(iii).

was passed, by the FISC itself.[81] In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information.[82] Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information,[83] although the foreign intelligence purpose of the collection does play a role in the court's Fourth Amendment analysis.[84]

In other respects, however, the FISC's role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702's statutory requirements and limitations.[85] With respect to the targeting procedures, the FISC must

---

80 *See, e.g.*, Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation, Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, at 9 (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf.

81 Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

82 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. *See* Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

83 50 U.S.C. § 1881a(i)(2).

84 Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

85 50 U.S.C. § 1881a(d)(2), (e)(2), (i)(1)(A).

C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit.[122] The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs "upstream" in the flow of communications between communication service providers.[123]

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA's minimization procedures. [124] CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways.[125] Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.[126]

---

122 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.").

123 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

124 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4.

125 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 27 (statement of Rajesh De, General Counsel, NSA).

126 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29.

1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector.[127] The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection.[128] Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition.[129] The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely "about" the tasked telephone number.[130]

2. Upstream Collection of Internet "Transactions"

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.[131] And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.[132]

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet

---

127 PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *id*. at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

128 NSA DCLPO REPORT, *supra*, at 6.

129 PCLOB March 2014 Hearing Transcript, *supra*, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

130 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5.

131 NSA DCLPO REPORT, *supra*, at 5-6.

132 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

communications, what is referred to as the "Internet backbone."[133] The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.[134]

Upstream collection acquires Internet transactions that are "to," "from," or "about" a tasked selector.[135] With respect to "to" and "from" communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an "about" communication. An "about" communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication.[136] If the NSA therefore applied its targeting procedures to task email address "JohnTarget@example.com," to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name "John Target." In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC's reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

---

133 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4.

134 Bates October 2011 Opinion, *supra*, at 73, 2011 WL 10945618, at *26.

135 *See, e.g.*, October 2011 Opinion, *supra*, at 15-16, 2011 WL 10945618, at *5-6 (describing the government's representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

136 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement") (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf; PCLOB March 2014 Hearing Transcript, *supra*, at 55.

III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications "selector," such as an email address or telephone number — the government acquires only those communications involving that particular selector.[474]

Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ and the ODNI ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA court does not approve individual targeting decisions or review them after they are made.

Although the "persons" who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,[475] the government is not exploiting any legal ambiguity by "targeting" an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.[476] In other words, selectors are always

---

474 See pages 20-23 and 32-33 of this Report.

475 *See* 50 U.S.C. §§ 1801(m), 1881a(a).

476 The NSA's "upstream collection" (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, "transactions") that contain a tasked selector go into government databases. See pages 36-41 of this Report.

While we believe that the measures taken by the NSA to exclude wholly domestic "about" communications may be reasonable in light of current technological limits, they are not perfect.[506] Even where both parties to a communication are located in the United States, in a number of situations the communication might be routed internationally, in which case it could be acquired by the NSA's upstream collection devices.[507] There are reasons to suppose that this occurs rarely, but presently no one knows how many wholly domestic communications the NSA may be acquiring each year as a result of "about" collection.[508]

The more fundamental concern raised by "about" collection is that it permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications.[509] This practice fundamentally differs from "incidental" collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target's communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples' communications — the government simply is acquiring the target's communications. In "about" collection, by contrast, the NSA's

---

506 December 2011 Joint Statement, *supra*, at 7 (acknowledging that the NSA's efforts "are not perfect").

507 *See generally* Bates October 2011 Opinion, *supra*, at 34, 2011 WL 10945618, at *11.

508 Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting "MCTs" (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to "about" collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in "about" collection "should be smaller — and certainly no greater — than potentially encountering wholly domestic communications within MCTs." *Id*. This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency's "about" collection might equal the percentage of wholly domestic communications within its collection of "MCTs," leading to an estimate of as many as 46,000 wholly domestic "about" communications acquired each year. *Id*. We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic "about" communications matches the number of wholly domestic MCTs, but the fact remains that the NSA cannot say how many domestic "about" communications it may be obtaining each year.

509 *See* December 2011 Joint Statement, *supra*, at 7 ("[U]pstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant."); The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4 ("Upstream collection . . . lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties.").

collection devices can acquire communications to which the target is not a participant, based at times on their contents.[510]

Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.[511] Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.[512] And without the ability to engage in inspection of this sort, nothing akin to "about" collection could feasibly occur with respect to such traditional forms of communication. Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them.

The government values "about" communications for the unique intelligence benefits that they can provide. Although we cannot discuss the details in an unclassified public report, the moniker "about" collection describes a number of distinct scenarios, which the government has in the past characterized as different "categories" of "about" collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.[513] In some instances, the targeted person actually is a participant to the communication (using a different communications selector than the one that was "tasked" for collection), and so the term "about" collection may be misleading.[514] In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.

---

510 *See* December 2011 Joint Statement, *supra*, at 7.

511 *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

512 *See Katz v. United States*, 389 U.S. 347 (1967).

513 Such communications include "any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the . . . previously identified categories of 'about communications[.]'" Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

514 The term *"about" communications* was originally devised to describe communications that were "about" the selectors of targeted persons — meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are "about" the targeted persons. References to targeted *persons* do not themselves lead to "about" collection; only references to the communications *selectors* of targeted persons lead to "about" collection.

internal agency reviews to ensure that the new targeting procedures have been adopted by its analysts. The executive branch compliance audits should also be modified to reflect the new targeting procedures and to include more rigorous scrutiny of whether valid foreign intelligence purpose determinations are being properly articulated.

II. U.S. Person Queries

Recommendation 2: The FBI's minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters.

When an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice, pursuant to the Attorney General Guidelines for Domestic FBI Operations, to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation. The databases queried may include information collected under various FISA authorities, including data collected under Section 702. The FBI's rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI's work concerns U.S. persons. If a query leads to a "hit" in the FISA data (i.e., if a communication is found within a repository of Section 702 data that is responsive to the query), then the agent or analyst is alerted to the existence of the hit. If the agent or analyst has received training on how to handle FISA-acquired materials, he or she is able to view the Section 702 data that was responsive to the query; however, if the agent or analyst has not received FISA training he or she is merely alerted to the existence of the information but cannot access it. The agent or analyst would have to contact a FISA-trained agent or analyst and ask him or her to review the information.

Even though FBI analysts and agents who solely work on non–foreign intelligence crimes are not *required* to conduct queries of databases containing Section 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when

the minimization procedures are presented to the court for approval with the government's next recertification application.

In light of the privacy and civil liberties implications of using Section 702 information, collected under lower thresholds and for a foreign intelligence purpose, in the FBI's pursuit of non–foreign intelligence crimes, the Board believes it is appropriate to place some additional limits on what can be done with Section 702 information. Members of the Board differ on the nature of the limitations that should be placed on the use of that information. Board Members' proposals and a brief explanation of the reasoning supporting each are stated below, with elaboration in the two separate statements.

Additional Comment of Chairman David Medine and Board Member Patricia Wald

For acquisitions authorized under Section 702, FISA permits the FBI for law enforcement purposes, to retain and disseminate evidence of a crime. However, there is a difference between obtaining a U.S. person's communications when they are in plain view as an analyst reviews the target's communications, and the retrieval of a U.S. person's communications by querying the FBI's Section 702 holdings collected over the course of years.[545] Therefore, consistent with our separate statement regarding Recommendation 3, we believe that U.S. persons' privacy interests regarding 702 data should be protected by requiring that each identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, other than in exigent circumstances. The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime. As discussed in more detail in our separate statement, this judicial review would not be necessary for U.S. persons who are already suspected terrorists and subject to surveillance under other government programs.

Additional Comment of Board Members Rachel Brand and Elisebeth Collins Cook

As explained in our separate statement, we would support a requirement that an analyst conducting a query in a non–foreign intelligence criminal matter obtain supervisory approval before accessing any Section 702 information that was responsive to the query. We would also support a requirement of higher-level Justice Department approval, to the extent not already required, before Section 702 information could be used

---

[545] On June 25, 2014, the United States Supreme Court ruled unanimously that a search of a cell phone seized by the police from an individual who has been arrested required a warrant. *Riley v. California*, No. 13-132, 2014 WL 2864483 (U.S. June 25, 2014). The Court distinguished between reviewing one record versus conducting an extensive records search over a long period: "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." *Id.* at *18. Likewise, observing evidence of a crime in one email does not justify conducting a search of an American's emails over the prior five years to or from everyone targeted under the Section 702 program.

EXHIBIT B

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN
Overview

OR

*The SIGAD Used **Most** in NSA Reporting*
Overview

[redacted] PRISM Collection Manager, S35333

April 2013

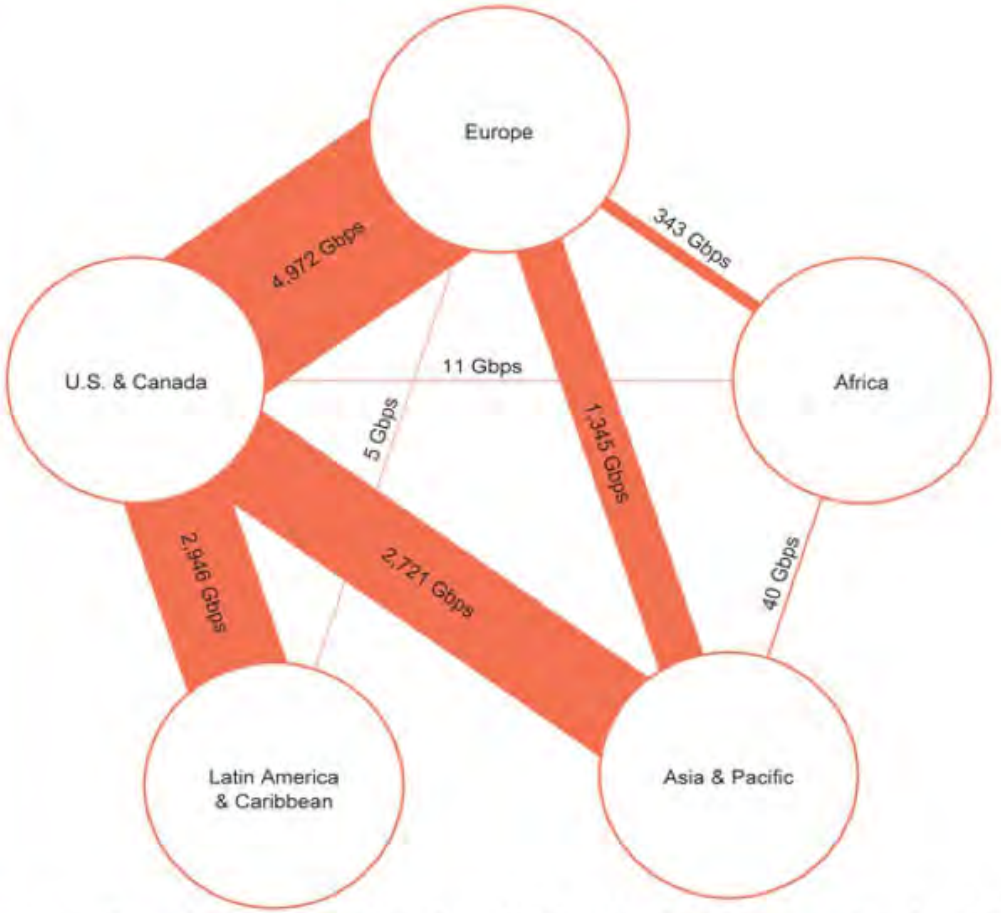
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone

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



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

PRISM

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

(TS//SI//NF) FAA702 Operations

Why Use Both: PRISM vs. Upstream

	PRISM	Upstream
DNI Selectors	✓ 9 U.S. based service providers	✓ Worldwide sources
DNR Selectors	⊘ Coming soon	✓ Worldwide sources
Access to Stored Communications (Search)	✓	⊘
Real-Time Collection (Surveillance)	✓	✓
"Abouts" Collection	⊘	✓
Voice Collection	✓ Voice over IP	✓
Direct Relationship with Comms Providers	⊘ Only through FBI	✓

EXHIBIT C

SECRET//SI//REL USA, GBR

(U//FOUO) WINDSTOP/2P
System Highlights

MUSCULAR

- Minor circuit move, not collection suite move (so-2013-00762)
- XKS FP updates across TU systems / NArchive throttle update

INCENSER

- INCS4 config issue (uo-2013-00471)

SECRET//SI//REL USA, GBR

Speaker's Notes

From Feb 28 2013: Proposed/imminent latest DO/Volume reduction: Narchive

BLUF: Requested S2 concurrence at S2 TLC on 25 Feb with partial throttling of content from Yahoo, Narchive email traffic which contains data older than 6 months from MUSCULAR. Numerous S2 analysts have complained of its existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4th of the total daily collect).

Background: Since July of 2012, Yahoo has been transferring entire email accounts using the Narchive data format (a proprietary format for which NSA had to develop custom demultiplexers). To date, we are unsure why these accounts are being transferred – movement of individuals, backup of data from overseas servers to US servers, or some other reason. There is no way currently to predict if an account will be transferred via Yahoo Narchive.

Currently, Narchive traffic is collected and forwarded to NSA for memorialization in any quantity only from DS-200B. On any given day, Narchive traffic represents 25% (15GB) of DS-200B's daily PINWALE content allocation (60GB currently). DS-200B is scheduled to be upgraded in the summer of 2013; it is likely that memorialized Narchive traffic, if still present in the environment, will grow proportionally (i.e. double now, to 30 GB/day).

Narchive traffic is mailbox formatted email, meaning unlike Yahoo webmail, any attachments present would be collected as part of the message. This is a distinct advantage. However, it has not been determined what causes an Narchive transfer of an account, so these messages are rarely collected "live".

Based on analysis of Narchive email data by [redacted] and [redacted], we were able to indentify statistics for the original communications date for Narchive email messages collected:

< 30 days	1118	11%
> 30 days, < 90 days	1758	17%
> 90 days < 180 days	1302	13%
> 180 days, < 1 year	2592	26%
> 1years, < 5 years	3084	31%
> 5years	154	>1%

Numerous target offices have complained about this collection "diluting" their workflow. One argument for keeping it is that it provides a retrospective look at target activity – this argument is hampered by a) the unreliable and non-understood nature of when the transfer occurs for an account, and b) that FISA restrospective collection would retrieve the exact same data "on demand".

SSO Optimization believes that while this is "valid" collection of content, the sheer volume and the age – coupled with the unpredictable nature of Narchive activity – makes collecting older data a less desirable use of valuable resources. 59% of Narchive email collected was originally sent and received more than 180 days after collection. This represents about 8.9 GB a day of "less desirable" collection – long term allocation that could be easily filled with more timely, useful FI from this lucrative SSO site. As always with our optimization, the data would still be available at the site store for SIGDEV. This would not impact metadata extraction.

Past DO volume reduction efforts:
Webmail OAB- Leap day 2012: the original defeat only targeted gmail, yahoo, and hotmail webmail protocol
FB buddylist sampling since last year

Today: FB OAB defeat/atxks/facebook/ownerless_addressbook : this is a JSON addressbook

EXHIBIT D

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

JOINT STATEMENT OF

LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
FOR NATIONAL SECURITY
U.S. DEPARTMENT OF JUSTICE

JOHN C. (CHRIS) INGLIS
DEPUTY DIRECTOR
NATIONAL SECURITY AGENCY

ROBERT S. LITT
GENERAL COUNSEL
OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING CONCERNING
"FISA AMENDMENTS ACT REAUTHORIZATION"

PRESENTED ON
DECEMBER 8, 2011

[redacted]

Joint Statement of

Lisa O. Monaco
Assistant Attorney General
for National Security
U.S. Department of Justice

John C. (Chris) Inglis
Deputy Director
National Security Agency

Robert S. Litt
General Counsel
Office of Director of National Intelligence

Before the
Permanent Select Committee on Intelligence
United States House of Representatives

At a Hearing Concerning
"FISA Amendments Act Reauthorization"

Presented on
December 8, 2011

[redacted]

[redacted]

[redacted]

[redacted]

(U) **Recent FISC Opinion**

~~(TS//SI//NF)~~ On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. *In re DNI/AG Certification 2009-C, et. al.*, [redacted], Mem. Op. The FISC approved most of the Government's submission. It upheld NSA's and FBI's targeting procedures, CIA's and FBI's minimization procedures, and most of NSA's minimization procedures. Nevertheless, the FISC denied in part the Government's requests because of its concerns about the rules governing the retention of certain non-targeted Internet communications acquired through NSA's upstream collection. The FISC's exhaustive analysis of the Government's submission, like its other decisions, refutes any argument that the court is a "rubber stamp," and demonstrates the rigorous nature of the oversight it conducts.

~~(TS//SI//NF)~~ As described above, upstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant. In doing so, NSA uses [redacted] that are reasonably designed to screen out communications that are wholly domestic in nature, in accordance with section 702's requirements. Although reasonably designed to accomplish this result, [redacted] are not perfect. In addition, upstream collection devices acquire Internet "transactions" that include tasked selectors. Such a transaction may consist of a single communication (a "single-communication transaction," or SCT) or multiple communications sent in a single transaction (a "multi-communication transaction," or MCT) [redacted] In such instances, upstream collection acquires the entire MCT, which in all cases will include a communication to, from, or about a tasked selector but in some cases may also include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship, to the targeted selector. Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information. Based on a sample reviewed by NSA, the percentage of such communications is very small (about .02%), but given the volume of the upstream collection, the FISC concluded that the actual number of such communications may be in the tens of thousands annually.

~~(TS//SI//NF)~~ The FISC upheld NSA's continued upstream acquisition of Internet communications under section 702 even though it includes the unintentional acquisition of wholly domestic communications and the incidental acquisition of MCTs that may contain one or more individual communications that are not to, from, or about the tasked selector. *See id.* at 74, 78-79. The FISC also reaffirmed that the acquisition of foreign intelligence information under section 702 falls within the foreign intelligence exception to the warrant requirement of the Fourth Amendment, and confirmed that nothing had disturbed its "prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures." *Id.* at 69.

~~(TS//SI//NF)~~ The FISC determined, however, that the minimization procedures governing *retention* of MCTs were inconsistent with the requirements of section 702. The FISC found that the Government had not fully explored options regarding data retention that would be more protective of U.S. persons, and that the FISC thus could not determine that the Government's minimization procedures satisfied FISA's requirement that such procedures be "reasonably designed" to minimize the retention of protected U.S. person information. The FISC further held that, although the Fourth Amendment's warrant requirement was not implicated, in light of NSA's proposed procedures for handling MCTs, NSA's proposed acquisition and minimization procedures did not satisfy the Fourth Amendment's reasonableness requirement. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment," and suggested a number of possibilities as to how this might be done. *Id.* at 61-63, 78-80.

~~(TS//SI//NF)~~ On October 31, 2011, after extensive consultations among the Department, ODNI, and NSA, the Attorney General submitted amended minimization procedures to the FISC addressing the deficiencies noted by the court. These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. On balance, NSA believes that the impact of these procedures on operations is acceptable as a necessary requirement in order to continue upstream collection, and that these procedures will allow for continued useful intelligence collection and analysis. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements."

(U) The Government has provided copies of the opinions and the filings by the Government to this Committee, and the Government will continue to inform the Committee about developments in this matter.

EXHIBIT E

1999
International Telecommunications Data

(Filed as of October 31, 2000)

December 2000

Linda Blake
Jim Lande

Industry Analysis Division
Common Carrier Bureau
Federal Communications Commission
Washington, DC 20554

This report is available for reference in the FCC's Reference Information Center at 445 12th Street, S.W., Courtyard Level. Copies may be purchased by calling International Transcription Services, Inc., (ITS) at (202) 857-3800. The report can be downloaded [file names: 4361-F99.ZIP or 4361-F99.PDF] from the **FCC-State Link** internet site at http://www.fcc.gov/ccb/stats on the World Wide Web.

Figure 9
International Message Telephone Traffic and Revenues
for the Three Largest International Carriers

	U.S. Billed Traffic			All Traffic that Originates or Terminates in the U.S.		
	Number of Minutes (000,000)	U.S. Carrier Revenue ($000,000)	Billed Revenue per Minute	Number of Minutes (000,000)	U.S. Carrier Retained Revenue ($000,000)	Net of Settlements Revenue per Minute
AT&T						
1991	6,596	$6,962	$1.06	10,020	$4,279	$0.43
1992	7,039	$7,314	$1.04	10,741	$4,814	$0.45
1993	7,201	$7,482	$1.04	10,938	$4,979	$0.46
1994	8,040	$7,984	$0.99	11,807	$5,229	$0.44
1995	8,831	$8,425	$0.95	12,778	$5,634	$0.44
1996	9,546	$8,559	$0.90	13,563	$5,705	$0.42
1997	10,331	$8,351	$0.81	14,529	$5,786	$0.40
1998	10,452	$7,533	$0.72	15,113	$5,332	$0.35
1999	10,900	$6,755	$0.62	15,944	$4,921	$0.31
MCI *						
1991	1,600	$1,487	$0.93	2,450	$958	$0.39
1992	2,101	$2,065	$0.98	3,163	$1,360	$0.43
1993	2,857	$2,779	$0.97	4,175	$1,789	$0.43
1994	3,529	$2,952	$0.84	5,206	$1,790	$0.34
1995	4,486	$3,968	$0.88	6,350	$2,402	$0.38
1996	5,372	$3,550	$0.66	7,496	$1,772	$0.24
1997	5,913	$4,243	$0.72	8,216	$2,634	$0.32
1998	7,195	$4,298	$0.60	10,257	$2,745	$0.27
1999	8,306	$5,056	$0.61	11,396	$3,489	$0.31
Sprint						
1991	728	$604	$0.83	1,139	$407	$0.36
1992	946	$786	$0.83	1,424	$520	$0.37
1993	1,181	$1,048	$0.89	1,730	$706	$0.41
1994	1,490	$1,229	$0.82	2,140	$742	$0.35
1995	1,772	$1,289	$0.73	2,480	$741	$0.30
1996	2,745	$1,493	$0.54	4,060	$672	$0.17
1997	2,794	$1,478	$0.53	4,505	$822	$0.18
1998	2,916	$1,421	$0.49	4,795	$922	$0.19
1999	3,640	$1,379	$0.38	5,507	$825	$0.15
WorldCom, Inc.						
1991	3	$2	$0.52	4	$1	$0.26
1992	12	$10	$0.82	21	$6	$0.29
1993	92	$64	$0.70	132	$27	$0.21
1994	278	$124	$0.45	362	$38	$0.10
1995	544	$291	$0.53	798	$144	$0.18
1996	846	$364	$0.43	1,137	$100	$0.09
1997	1,400	$500	$0.36	1,842	$114	$0.06
1998	-	-	-	-	-	-
1999	-	-	-	-	-	-

* MCI for years 1991-1997, MCI WorldCom, Inc. thereafter.

EXHIBIT F

Liberty and Security in a Changing World

12 December 2013

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies

During the Cold War, ordinary Americans used the telephone for many local calls, but they were cautious about expensive "long-distance" calls to other area codes and were even more cautious about the especially expensive "international" phone calls. Many people today, by contrast, treat the idea of "long-distance" or "international" calls as a relic of the past. We make international calls through purchases of inexpensive phone cards or free global video services. International e-mails are cost-free for users.

The pervasively international nature of communications today was the principal rationale for creating Section 702 and other parts of the FISA Amendments Act of 2008. In addition, any communication on the Internet might be routed through a location outside of the United States, in which case FISA does not apply and collection is governed under broader authorities such as Executive Order 12333. Today, and unbeknownst to US users, websites and cloud servers may be located outside the United States. Even for a person in the US who never knowingly sends communications abroad, there may be collection by US intelligence agencies outside of the US. [160] The cross-border nature of today's communications suggests that when decisions are made about foreign surveillance, there is a need for greater consideration of policy goals involving the protection of civilian commerce and individual privacy.

[160] *See* Jonathan Mayer, "The Web is Flat" Oct. 30, 2013 (study showing "pervasive" flow of web browsing data outside of the US for US individuals using US-based websites), available at http://webpolicy.org/2013/10/30/the-web-is-flat/.

STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
JULIA BERMAN
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 7132
Washington, D.C. 20001
Phone: (202) 514-2205; Fax: (202) 616-8470

Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-4373-JSW Case No. 4:07-cv-00693-JSW **DECLARATION OF JAMES J. GILLIGAN IN SUPPORT OF GOVERNMENT DEFENDANTS' REPLY BRIEF REGARDING COMPLIANCE WITH PRESERVATION ORDERS**
CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No hearing scheduled Oakland Courthouse Courtroom 5, 2nd Floor The Honorable Jeffrey S. White

I, James J. Gilligan, hereby declare:

1. I am the Special Litigation Counsel for the United States Department of Justice, Civil Division, Federal Programs Branch, and attorney of record for the official capacity Government Defendants in the above-captioned cases. The statements made herein are based on my personal knowledge, and on information made available to me in the course of my duties and responsibilities as counsel for the official capacity Government Defendants in these cases.

2. Filed with this declaration, as Exhibits A through F in support of the Government Defendants' Reply Brief Regarding Compliance with Preservation Orders, are true and correct copies of the following documents:

a. Exhibit A, NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 ("Civil Liberties and Privacy Office Report"), dated Apr. 16, 2014;

b. Exhibit B, Intelligence Community's Collection Programs under Title VII of the Foreign Intelligence Surveillance Act ("IC's Collection Programs");

c. Exhibit C, Office of the Director of National Intelligence, Statistical Transparency Report Regarding use of National Security Authorities, dated June 26, 2014;

d. Exhibit D, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("ODNI Fact Sheet"), dated June 8, 2013;

e. Exhibit E, The National Security Agency: Missions, Authorities, Oversight and Partnerships, dated Aug. 9, 2013; and

f. Exhibit F, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, dated Oct. 31, 2011 ("Minimization Procedures").

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on June 27, 2014, at Washington, D.C.

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

EXHIBIT B

(U) The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act

(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. 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 THOSE WHO ACCESS THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

(U) Introduction

(S//NF) Section 702 of the Foreign Intelligence Surveillance Act (FISA), added by the FISA Amendments Act (FAA) of 2008, has proven to be a critical tool in the Government's efforts to acquire foreign intelligence necessary to protect the Nation's security, while at the same time establishing rigorous safeguards to protect the privacy interests of U.S. persons. The FAA has significantly enhanced the capability of the Intelligence Community to collect information about [redacted]. Section 702, along with other important provisions of the FAA, will expire at the end of this year unless reauthorized by Congress. Reauthorization is the top legislative priority of the Intelligence Community. This paper provides an overview of all of the expiring provisions of the FAA, including section 704, which provides greater protection for collection activities directed against U.S. persons overseas than existed before passage of the FAA. The principal focus of the paper is section 702, including the extensive oversight of its use and the importance of this authority to our national security. An attachment contains examples of the valuable intelligence section 702 collection has provided.

(U) I. Overview of Section 702

(U) Legal Requirements

(S//NF) Many terrorists and other foreign intelligence targets abroad use communications services based in this country, [redacted]

Classified By: 2381928
Declassify On: 20320108
Derived From: NSA/CSSM 1-52

[redacted] These provisions require a finding of probable cause that the overseas target is a foreign power or an agent of a foreign power, such as an international terrorist organization, and that the target is using or about to use the targeted facility, such as a telephone number or e-mail account. The Attorney General, and subsequently the Foreign Intelligence Surveillance Court (FISC), must approve each application. In effect, the Intelligence Community had to treat the overseas foreign target the same way as a U.S. person or person in the United States and obtain an individual order, based on a finding of probable cause by a neutral magistrate, even though the target was neither a U.S. person nor a person in the United States. Non-U.S. persons outside the United States generally are not entitled to the protections of the Fourth Amendment. Accordingly, the Constitution does not require this burdensome practice.

(S//NF) Section 702 remedies these shortcomings and permits the Government to acquire, safely and efficiently from providers in the United States, communications where non-U.S. persons located abroad are targeted for the purpose of acquiring foreign intelligence information. At the same time, it provides a comprehensive regime of oversight by all three branches of Government to protect the constitutional and privacy interests of Americans.

(U//FOUO) Under section 702, instead of issuing individual orders, the FISC, which is comprised of federal judges from around the country appointed by the Chief Justice of the Supreme Court, approves annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that identify broad categories of foreign intelligence which may be collected. The statute stipulates several criteria for collection. First, the Attorney General and the DNI must certify that a significant purpose of an acquisition is to obtain foreign intelligence information. Second, an acquisition may intentionally target only non-U.S. persons. Third, an acquisition may not intentionally target any person known at the time of the acquisition to be in the United States. Fourth, an acquisition may not target a person outside the United States for the purpose of targeting a particular, known person in this country. Fifth, section 702 protects domestic communications by prohibiting the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States. Finally, any acquisition must be consistent with the Fourth Amendment. The certifications are the legal basis for targeting specific individuals overseas and, based on the certifications, the Attorney General and the DNI can direct communications providers in this country to assist the Government in acquiring these targets' communications.

(U) Because when originally passed Congress understood that U.S.-person communications would incidentally be acquired when targeting foreign communications, to ensure compliance with these provisions, section 702 requires the Attorney General, in consultation with the DNI, to adopt targeting and minimization procedures. Under the statute, the targeting procedures must be reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of purely domestic communications. The minimization procedures govern how the Intelligence Community treats the identities of any U.S. persons whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S.

persons that is acquired. These minimization procedures must meet the same standard as the minimization procedures required by other provisions of FISA. The FISC reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the Fourth Amendment, and the appropriate congressional committees receive copies of them. By approving the certifications submitted by the Attorney General and the DNI as well as the targeting and minimization procedures, the FISC plays a vital role in ensuring that acquisitions under section 702 are conducted in a lawful and appropriate manner.

(U) **Implementation**

(S//NF) Currently, the Attorney General and the DNI have authorized the acquisition of foreign intelligence information under section 702 [redacted] The Attorney General and the DNI must resubmit these certifications to the FISC for review and renewal at least once a year. Using these certifications, Intelligence Community elements participate in the tasking of selectors for telephony, as well as electronic communications accounts, such as e-mail addresses.

(S//NF) NSA takes the lead in targeting and tasks both telephone and electronic communications selectors to acquire communications [redacted]. NSA's targeting procedures require that there be an appropriate foreign intelligence purpose for the acquisition and that the selector be used by a non-U.S. person reasonably believed to be located outside the United States. To determine the location of a user, an analyst must, as appropriate, examine the lead information about the potential target or selector; [redacted]

(S//NF) [redacted]. Because NSA has already made a "foreignness" determination for these selectors in accordance with its FISC-approved targeting procedures, FBI's targeting role differs from that of NSA. FBI is not required to second-guess NSA's targeting determinations. It must, however, review and understand NSA's targeting determinations, [redacted].

(TS//SI//NF) Once a target has been approved, NSA uses two means to acquire [redacted] electronic communications. First, [redacted], it acquires such communications directly from U.S.-based ISPs. This is known as PRISM collection. Using PRISM, NSA currently collects against approximately [redacted] selectors at any given time.

(TS//SI//NF) Second, in addition to collection directly from ISPs, NSA collects telephone and electronic communications as they transit the Internet "backbone" within the United States. This

is known as "upstream" collection [redacted], the volume of communications acquired upstream is much smaller than that obtained through PRISM. In June 2011, for example, it made up only about 11% of the overall section 702 volume. [redacted]

~~(TS//SI//NF)~~ Upstream collection enables NSA to target terrorists [redacted] It also lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties. Finally, NSA obtains certain international or foreign telephone communications from this collection.

~~(TS//SI//NF)~~ Once acquired, all communications are routed to NSA. NSA also can designate the communications from specified selectors acquired through PRISM collection to be "dual-routed" to other Intelligence Community elements. Each agency that receives the collection has its own minimization procedures that have been approved by the FISC and may retain and disseminate communications acquired under section 702 only in accordance with those procedures. In general, before an agency may disseminate information identifying a U.S. person, the information must reasonably appear to be foreign intelligence or evidence of a crime, or necessary to understand or assess foreign intelligence information.

(U) **Compliance and Oversight**

(U) The Executive Branch is committed to ensuring that the Intelligence Community's use of section 702 is consistent with the law, the FISC's orders, and the protection of the privacy and civil liberties of Americans. The Intelligence Community, the Department of Justice, and the FISC all play a critical role in overseeing the use of this provision. In addition, the Intelligence and Judiciary Committees carry out essential oversight, which is discussed separately in section IV below.

~~(S//NF)~~ First, components in each agency, including operational components and agency Inspectors General, conduct extensive oversight. Agencies using section 702 authority must report promptly to the Department of Justice and to the Office of the Director of National Intelligence (ODNI) incidents of noncompliance with the targeting or minimization procedures. Members of the joint oversight team from the National Security Division (NSD) of the Department of Justice and ODNI routinely review the agencies' targeting decisions. Currently, at least once every 60 days, NSD and ODNI conduct oversight of activities under section 702. The joint oversight team evaluates and where appropriate investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions.

~~(S//NF)~~ Using the reviews by NSD and ODNI personnel, the Attorney General and the DNI assess semi-annually, as required by section 702, compliance with the targeting and minimization procedures. These assessments are provided twice yearly to Congress. In general,

the assessments have found that agencies have "continued to implement the procedures . . . in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702." The number of compliance incidents has been small, with no indication of "any intentional attempt to circumvent or violate" legal requirements. Rather, agency personnel "are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States." *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2010 – May 31, 2011* at 2-3, 5. 21-22 (December 2011).

(U) The Intelligence Community and the Department of Justice use the reviews and oversight to evaluate whether changes to the procedures are needed, and what other steps may be appropriate under section 702 to protect the privacy of Americans. The Government also provides the joint assessments, the major portions of the semi-annual reports, and a separate quarterly report to the FISC. Taken together, these measures provide robust oversight of the Government's use of this authority.

~~(TS//SI//NF)~~ One recent event demonstrates both how this oversight regime works and how challenging collection can be in the complex and rapidly evolving Internet environment. On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. Although the FISC upheld the bulk of the Government's submission, it denied in part the Government's requests to reauthorize the certifications because of its concerns about the rules governing the retention of certain non-targeted Internet communications -- so called multi-communication transactions or MCTs -- acquired through NSA's upstream collection. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards" in a manner that would satisfy its concerns, and suggested a number of possibilities as to how this might be done. In response to this opinion, the NSA, Department of Justice, and ODNI worked to correct the deficiencies identified by the Court. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to the 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements." These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. The Government's extensive efforts over several months to address this matter, and the FISC's exhaustive analysis of it, demonstrates how well the existing oversight regime works in ensuring that collection is undertaken in conformity with the statute and Court-approved procedures. This issue was also fully briefed to the appropriate congressional committees, again highlighting the important role that Congress plays in overseeing these vital intelligence activities.

(U) II. The Importance of Section 702 Collection

(S//NF) The Administration believes that a failure to renew this authority would result in a loss of critical foreign intelligence that cannot practicably be obtained through other methods.

(S//NF) To require an individualized court order, based on a finding of probable cause, before acquiring the communications of a non-U.S. person overseas who is believed to be involved in international terrorist activities or who is otherwise of foreign intelligence interest would have serious adverse consequences. Where the Intelligence Community has reason to believe that a non-U.S. person located overseas is connected to international terrorist activities, but does not have enough facts to establish probable cause to conclude that the target is acting as an agent of a foreign power, such a requirement could prevent the United States from acquiring significant intelligence. Even where the United States could, over time, amass additional information from other sources to establish probable cause, a requirement that such additional information be obtained and submitted to the FISC would result in delays in collection that could prove harmful. Second, even where the Intelligence Community has facts that establish probable cause that foreign targets are acting as foreign powers or agents of foreign powers, eliminating section 702's more flexible targeting system would significantly slow the Intelligence Community's ability to acquire important foreign intelligence information. This flexibility is critical in fast-moving threat scenarios. Significant additional resources would have to be devoted to preparing and processing the FISC applications and even then, given the number of selectors tasked, it is simply not feasible to obtain individualized orders on a routine basis for the thousands of foreign persons targeted under section 702. Intelligence would be lost. Moreover, failure to renew section 702 would require redirection of a substantial portion of the oversight resources of the Intelligence Community, the Department of Justice, and the FISC from their other important national security related work to the processing of FISA applications targeting non-U.S. persons overseas who are not entitled to Fourth Amendment protections under our Constitution. In contrast, section 702 increases the Government's ability to acquire important foreign intelligence information and to act quickly against appropriate foreign targets, without sacrificing constitutional protections for Americans.

(TS//SI//NF) Another major benefit of section 702 is that it has made collection against foreign targets located outside the United States possible from the relative safety of collection points in the United States. [redacted]

(TS//SI//NF) In sum, section 702 collection is a major contributor to the Intelligence Community's reporting on counterterrorism, [redacted] and other topics. Attached to this paper are several examples that demonstrate the broad range of important information that the Intelligence Community has obtained from section 702 collection.

(U) III. Other Provisions of the FAA

(U) In contrast to section 702, which focuses on foreign targets, section 704 addresses collection activities directed against U.S. persons overseas. Section 704 requires an individual order from the FISC in circumstances in which a U.S. person overseas has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." It also requires probable cause to believe that the targeted U.S. person is "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power." Previously, these activities were outside the scope of FISA and governed exclusively by section 2.5 of Executive Order 12333.[1] By requiring the approval of the FISC, section 704 provides additional protection for civil liberties.

(U) In addition to sections 702 and 704, the FAA added several other provisions to FISA. Section 701 provides definitions for the Act. Section 703 allows the FISC to authorize an application targeting a U.S. person outside the United States where the acquisition is conducted in this country. Like section 704, section 703 requires probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Section 705 allows the Government to obtain various authorities simultaneously. Section 709 clarifies that nothing in the FAA is intended to limit the Government's ability to obtain authorizations under other parts of FISA. The Government supports the reauthorization of these provisions.

(U) IV. Congressional Oversight

(U) The Executive Branch appreciates the need for regular and meaningful Congressional oversight of the use of section 702 and the other provisions of the FAA. Twice a year, the Attorney General must "fully inform, in a manner consistent with national security," the Intelligence and Judiciary Committees about the implementation of the FAA. Additionally, with respect to section 702, the report must include copies of certifications and directives and copies of significant pleadings and FISC opinions and orders. It also must describe compliance matters, any use of emergency authorities, and the FISC's review of the Government's pleadings. With respect to sections 703 and 704, the report must include the number of applications made, and the number granted, modified, or denied by the FISC.

(U) Section 702 also requires the Attorney General and the DNI to provide to the Intelligence and Judiciary Committees their assessment of compliance with the targeting and minimization procedures, described above. In addition, the Government has substantial reporting requirements imposed by FISA under which it has provided Congress information to ensure effective congressional oversight. The Government has informed the Intelligence and Judiciary Committees of acquisitions authorized under section 702; reported, in detail, on the results of the

---

[1] (U) Since before the enactment of the FAA, section 2.5 of Executive Order 12333 has required the Attorney General to approve the use by the Intelligence Community against U.S. persons abroad of "any technique for which a warrant would be required if undertaken for law enforcement purposes." The Attorney General must find that there is probable cause to believe that the U.S. person is a foreign power or an agent of a foreign power. The provisions of section 2.5 continue to apply to these activities, in addition to the requirements of section 704.

reviews and on compliance incidents and remedial efforts; made all written reports on these reviews available to the Committees; and provided summaries of significant interpretations of FISA, as well as copies of relevant judicial opinions and pleadings.

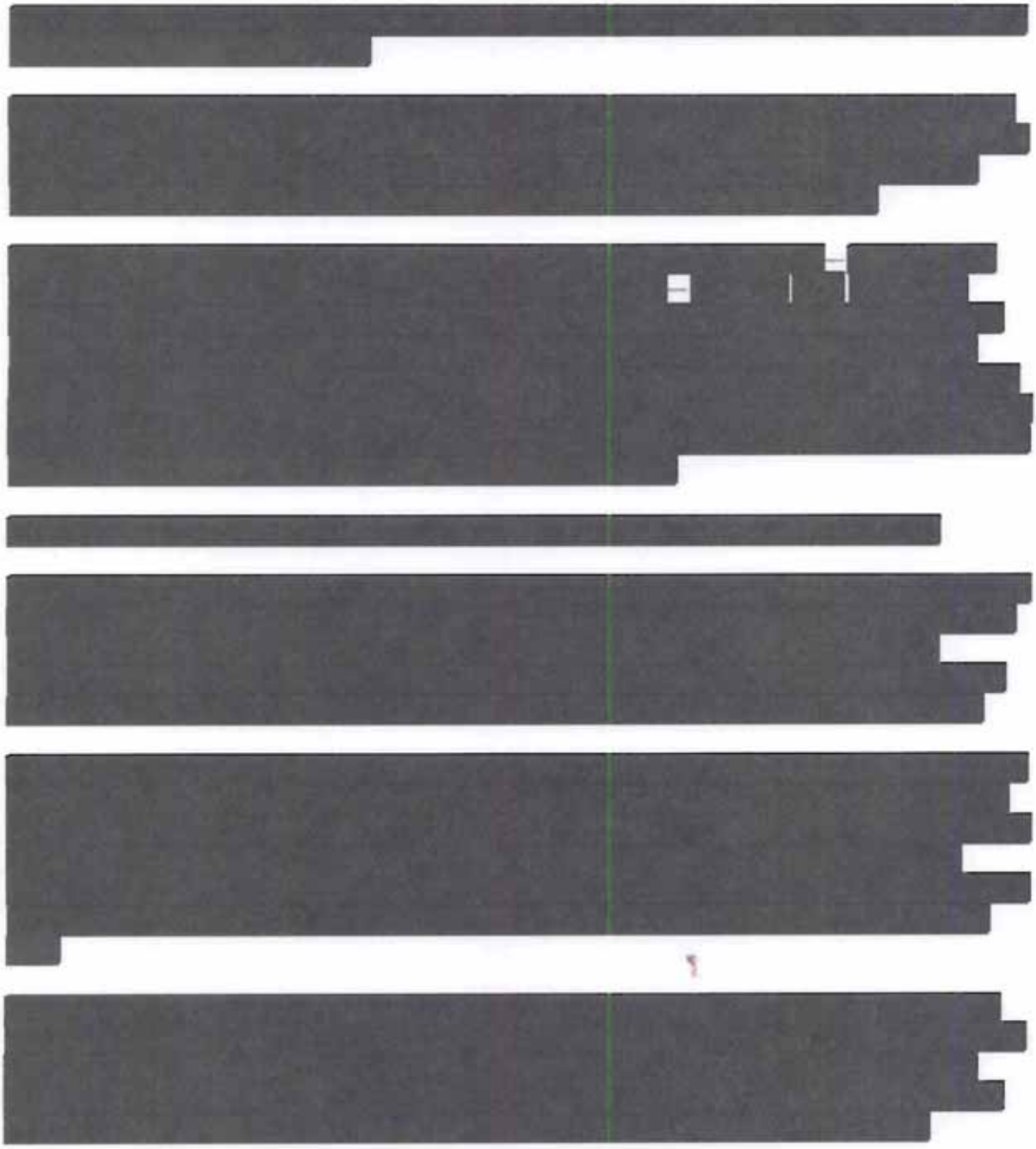
(U) V. The Need for Reauthorization

(U) The Administration strongly supports the reauthorization of Title VII of FISA. The FAA was the product of bipartisan effort, and its enactment was preceded by extensive public debate. There is now a lengthy factual record on the Government's need for the FAA to acquire foreign intelligence information critical to the national security. There is also a lengthy record documenting the effectiveness of the oversight process in protecting the privacy and civil liberties of Americans. This extensive record demonstrates the proven value of these authorities, and the commitment of the Government to their lawful and responsible use.

(U) Reauthorization will ensure continued certainty for the rules used by agency employees and our private partners. The Intelligence Community has invested significant human and financial resources to enable its personnel and technological systems to acquire and review vital data quickly and lawfully. Our adversaries, of course, seek to hide the most important information from us. It is at best inefficient and at worst unworkable for agencies to develop new technologies and procedures and train employees, only to have a statutory framework subject to wholesale revision. This is particularly true at a time of limited resources. We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans. Our first priority, however, is reauthorization of these authorities in their current form. It is essential that these authorities remain in place without interruption—and without the threat of interruption—so that those who have been entrusted with their use can continue to protect our nation from its enemies.

Attachment
Value of Section 702 Collection

(U) Section 702 is a critical intelligence collection tool that has helped to protect national security. The following are "real-life" examples that demonstrate the broad range of important information that the Intelligence Community has obtained.



[redacted]

(S//NF) **Example 4: Najibullah Zazi**

(S//NF) The FBI's arrest in 2009 of Najibullah Zazi in Colorado, the disruption of his planned attack on the New York subway system, and his eventual guilty plea to terrorism charges were the direct result of section 702 coverage. NSA observed that an al Qa'ida external operations account, which was under section 702 coverage, sent an e-mail to Zazi in September 2009. That allowed NSA to pass Zazi's e-mail account, [redacted], and telephone number to the FBI. This initial report was based solely on section 702 collection. The report led to Zazi's identification and the discovery of purchases in Colorado that could be used in a terrorist attack, and ultimately to his arrest and the arrests of others involved in the plot. Thus section 702 facilitated the disruption of one of the most serious terrorist plots against the homeland since September 11th.

[redacted]

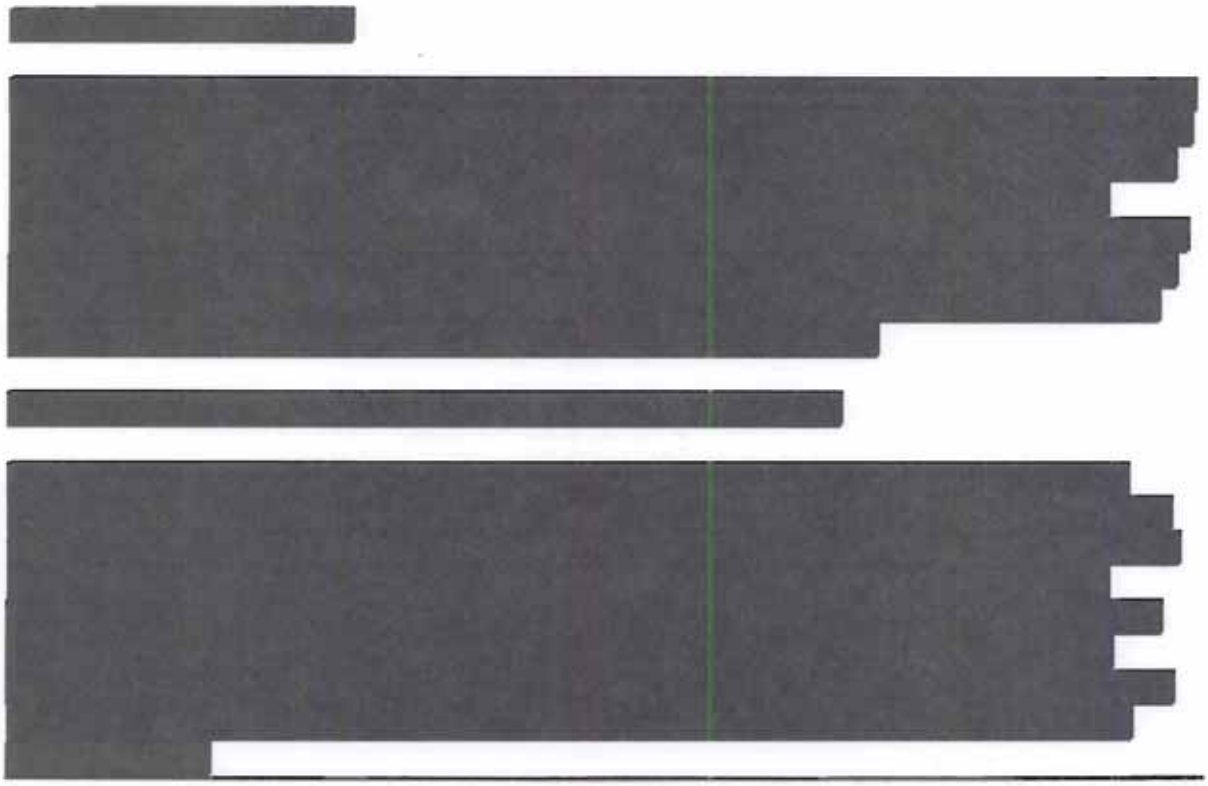


EXHIBIT F

~~TOP SECRET//COMINT//NOFORN//20320108~~

EXHIBIT B

MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

Section 1 - Applicability and Scope (U)

These National Security Agency (NSA) minimization procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be located outside the United States in accordance with section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"). (U)

If NSA determines that it must take action in apparent departure from these minimization procedures to protect against an immediate threat to human life (e.g., force protection or hostage situations) and that it is not feasible to obtain a timely modification of these procedures, NSA may take such action immediately. NSA will report the action taken to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such activity. (U)

For the purposes of these procedures, the terms "National Security Agency" and "NSA personnel" refer to 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 section 702 of the Act if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). (U)

Section 2 - Definitions (U)

In addition to the definitions in sections 101 and 701 of the Act, the following definitions will apply to these procedures:

(a) Acquisition means the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~TOP SECRET//COMINT//NOFORN//20310108~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization will be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States. All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications. ~~(S//SI)~~

(f) Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//SI)~~

(g) Internet transaction, for purposes of these procedures, means an Internet communication that is acquired through NSA's upstream collection techniques. An Internet transaction may contain information or data representing either a discrete communication [redacted] or multiple discrete communications [redacted] (TS//SI)

(h) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

(i) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(j) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S//SI)~~

(k) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

(1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be

positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with 8 U.S.C. § 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

Section 3 - Acquisition and Processing - General (U)

(a) Acquisition (U)

The acquisition of information by targeting non-United States persons reasonably believed to be located outside the United States pursuant to section 702 of the Act will be effected in accordance with an authorization made by the Attorney General and Director of National Intelligence pursuant to subsection 702(a) of the Act and will be conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. ~~(S//SI)~~

(b) Monitoring, Recording, and Processing (U)

(1) Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures. Except as provided for in subsection 3(c)(2) below, such inadvertently acquired communications of or concerning a United States person may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~

(2) Communications of or concerning United States persons that may be related to the authorized purpose of the acquisition may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, 6, and 8 of these procedures. ~~(C)~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(3) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S)~~

(4) As a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5, 6, and 8 of these procedures. ~~(S//SI)~~

(5) Processing of Internet Transactions Acquired Through NSA Upstream Collection Techniques ~~(TS//SI)~~

a. Notwithstanding any processing (e.g., decryption, translation) that may be required to render an Internet transaction intelligible to analysts, NSA will take reasonable steps post-acquisition to identify and segregate through technical means Internet transactions that cannot be reasonably identified as containing single, discrete communications where: the active user of the transaction (i.e., the electronic communications account/address/identifier used to send or receive the Internet transaction to or from a service provider) is reasonably believed to be located in the United States; or the location of the active user is unknown. ~~(TS//SI)~~

1. Internet transactions that are identified and segregated pursuant to subsection 3(b)(5)a. will be retained in an access-controlled repository that is accessible only to NSA analysts who have been trained to review such transactions for the purpose of identifying those that contain discrete communications as to which the sender and all intended recipients are reasonably believed to be located in the United States. ~~(TS//SI)~~

(a) Any information contained in a segregated Internet transaction [redacted] may not be moved or copied from the segregated repository or otherwise used for foreign intelligence purposes unless it has been determined that the transaction does not contain any discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States. Any Internet transaction that is identified and segregated pursuant to subsection 3(b)(5)a. and is subsequently determined to contain a discrete communication as to which the sender and all intended recipients are reasonably believed to be located in the United States will be destroyed upon recognition. ~~(TS//SI)~~

(b) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance the other applicable provisions of these procedures. ~~(TS//SI)~~

(c) Any information moved or copied from the segregated repository into repositories more generally accessible to NSA analysts will be marked, tagged, or otherwise identified as having been previously segregated pursuant to subsection 3(b)(5)a.

2. Internet transactions that are not identified and segregated pursuant to subsection 3(b)(5)a. will be processed in accordance with subsection 3(b)(5)b. below and handled in accordance with the other applicable provisions of these procedures.

b. NSA analysts seeking to use (for example, in a FISA application, intelligence report, or section 702 targeting) a discrete communication within an Internet transaction that contains multiple discrete communications will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~

1. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will first perform checks to determine the locations of the sender and intended recipients of that discrete communication to the extent reasonably necessary to determine whether the sender and all intended recipients of that communication are located in the United States. ~~(TS//SI)~~

2. If an NSA analyst seeks to use a discrete communication within an Internet transaction that contains multiple discrete communications, the analyst will assess whether the discrete communication is to, from, or about a tasked selector, or otherwise contains foreign intelligence information. ~~(TS//SI)~~

(a) If the discrete communication is to, from, or about a tasked selector, any U.S. person information in that communication will be handled in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~

(b) If the discrete communication is not to, from, or about a tasked selector but otherwise contains foreign intelligence information, and the discrete communication is not to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, that communication (including any U.S. person information therein) will be treated in accordance with the applicable provisions of these procedures. ~~(TS//SI)~~

(c) If the discrete communication is not to, from, or about a tasked selector but is to or from an identifiable U.S. person or a person reasonably believed to be located in the United States, the NSA analyst will document that determination in the relevant analytic repository or tool if technically possible or reasonably feasible. Such discrete communication cannot be used for any purpose other than to protect against an immediate threat to

~~TOP SECRET//COMINT//NOFORN//20310108~~

human life (e.g., force protection or hostage situations). NSA will report any such use to the Office of the Director of National Intelligence and to the National Security Division of the Department of Justice, which will promptly notify the Foreign Intelligence Surveillance Court of such use. ~~(TS//SI)~~

3. An NSA analyst seeking to use a discrete communication within an Internet transaction that contains multiple discrete communications in a FISA application, intelligence report, or section 702 targeting must appropriately document the verifications required by subsections 3(b)(5)b.1. and 2. above. ~~(TS//SI)~~

4. [redacted]

(6) Magnetic tapes or other storage media containing communications acquired pursuant to section 702 may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, will be limited to those selection terms reasonably likely to return foreign intelligence information. Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures. NSA will maintain records of all United States person identifiers approved for use as selection terms. The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph. ~~(S//SI)~~

(7) Further processing, retention and dissemination of foreign communications will be made in accordance with Sections 4, 6, 7, and 8 as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications will be made in accordance with Sections 4, 5, and 8 below. ~~(S//SI)~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(c) Destruction of Raw Data ~~(C)~~

(1) Telephony communications, Internet communications acquired by or with the assistance of the Federal Bureau of Investigation from Internet Service Providers, and other discrete forms of information (including that reduced to graphic or "hard copy" form such as facsimile, telex, computer data, or equipment emanations) that do not meet the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition, and may be retained no longer than five years from the expiration date of the certification authorizing the collection in any event. ~~(S//SI)~~

(2) Internet transactions acquired through NSA's upstream collection techniques that do not contain any information that meets the retention standards set forth in these procedures and that are known to contain communications of or concerning United States persons will be destroyed upon recognition. All Internet transactions may be retained no longer than two years from the expiration date of the certification authorizing the collection in any event. The Internet transactions that may be retained include those that were acquired because of limitations on NSA's ability to filter communications. Any Internet communications acquired through NSA's upstream collection techniques that are retained in accordance with this subsection may be reviewed and processed only in accordance with the standards set forth in subsection 3(b)(5) of these procedures. ~~(TS//SI)~~

(d) Change in Target's Location or Status ~~(S//SI)~~

(1) In the event that NSA determines that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person is in fact a United States person, the acquisition from that person will be terminated without delay. ~~(S//SI)~~

(2) Any communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of targeting was believed to be a non-United States person but was in fact a United States person, will be treated as domestic communications under these procedures. ~~(S//SI)~~

Section 4 - Acquisition and Processing - Attorney-Client Communications ~~(C)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment in the United States and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication will be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the communication containing that conversation will be segregated and the National Security

Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. Additionally, all proposed disseminations of information constituting United States person attorney-client privileged communications must be reviewed by the NSA Office of General Counsel prior to dissemination. ~~(S//SI)~~

Section 5 - Domestic Communications (U)

A communication identified as a domestic communication will be promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that: ~~(S)~~

(1) the communication is reasonably believed to contain significant foreign intelligence information. Such communication may be provided to the FBI (including United States person identities) for possible dissemination by the FBI in accordance with its minimization procedures; ~~(S)~~

(2) the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. Such communications may be retained by NSA for a reasonable period of time, not to exceed six months unless extended in writing by the Attorney General, to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes; ~~(S)~~

(3) the communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security vulnerability. Such communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such communications may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//SI)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//SI)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements; or ~~(S//SI)~~

(4) the communication contains information pertaining to a threat of serious harm to life or property. ~~(S)~~

Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may advise the FBI of that fact. Moreover, technical data regarding domestic communications may be retained and provided to the FBI and CIA for collection avoidance purposes. ~~(S//SI)~~

Section 6 - Foreign Communications of or Concerning United States Persons (U)

(a) Retention (U)

Foreign communications of or concerning United States persons collected in the course of an acquisition authorized under section 702 of the Act may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years from the expiration date of the certification authorizing the collection unless the Signals Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements;

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below; or

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. ~~(S//SI)~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 or 8 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise, dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) the communication or information indicates that the United States person may be:

a. an agent of a foreign power;

b. a foreign power as defined in Section 101(a) of the Act;

c. residing outside the United States and holding an official position in the government or military forces of a foreign power;

d. a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

e. acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material;

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information or the United States person's identity is necessary to understand or assess a communications security vulnerability, but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to the Act and the communication may relate to the foreign intelligence purpose of the surveillance; or

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in accordance with 50 U.S.C. §§ 1806(b) and 1825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document. (U)

(c) Provision of Unminimized Communications to CIA and FBI ~~(S//NF)~~

(1) NSA may provide to the Central Intelligence Agency (CIA) unminimized communications acquired pursuant to section 702 of the Act. CIA will identify to NSA targets for which NSA may provide unminimized communications to CIA. CIA will process any such unminimized communications received from NSA in accordance with CIA minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI//NF)~~

(2) NSA may provide to the FBI unminimized communications acquired pursuant to section 702 of the Act. The FBI will identify to NSA targets for which NSA may provide unminimized communications to the FBI. The FBI will process any such unminimized communications received from NSA in accordance with FBI minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, pursuant to subsection 702(e) of the Act. ~~(S//SI)~~

Section 7 - Other Foreign Communications (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

Section 8 - Collaboration with Foreign Governments ~~(S//SI)~~

(a) Procedures for the dissemination of evaluated and minimized information. Pursuant to Section 1.7(c)(8) of Executive Order No. 12333, as amended, NSA conducts foreign cryptologic liaison relationships with certain foreign governments. Information acquired pursuant to section 702 of the Act may be disseminated to a foreign government. Except as provided in subsection 8(b) of these procedures, any dissemination to a foreign government of information of or concerning a United States person that is acquired pursuant to section 702 may only be done in a manner consistent with subsections 6(b) and 7 of these NSA minimization procedures. ~~(S)~~

~~TOP SECRET//COMINT//NOFORN//20310108~~

(b) Procedures for technical or linguistic assistance. It is anticipated that NSA may obtain information or communications that, because of their technical or linguistic content, may require further analysis by foreign governments to assist NSA in determining their meaning or significance. Notwithstanding other provisions of these minimization procedures, NSA may disseminate computer disks, tape recordings, transcripts, or other information or items containing unminimized information or communications acquired pursuant to section 702 to foreign governments for further processing and analysis, under the following restrictions with respect to any materials so disseminated: ~~(S)~~

(1) Dissemination to foreign governments will be solely for translation or analysis of such information or communications, and assisting foreign governments will make no use of any information or any communication of or concerning any person except to provide technical and linguistic assistance to NSA. ~~(S)~~

(2) Dissemination will be only to those personnel within foreign governments involved in the translation or analysis of such information or communications. The number of such personnel will be restricted to the extent feasible. There will be no dissemination within foreign governments of this unminimized data. ~~(S)~~

(3) Foreign governments will make no permanent agency record of information or communications of or concerning any person referred to or recorded on computer disks, tape recordings, transcripts, or other items disseminated by NSA to foreign governments, provided that foreign governments may maintain such temporary records as are necessary to enable them to assist NSA with the translation or analysis of such information. Records maintained by foreign governments for this purpose may not be disseminated within the foreign governments, except to personnel involved in providing technical or linguistic assistance to NSA. ~~(S)~~

(4) Upon the conclusion of such technical or linguistic assistance to NSA, computer disks, tape recordings, transcripts, or other items or information disseminated to foreign governments will either be returned to NSA or be destroyed with an accounting of such destruction made to NSA. ~~(S)~~

(5) Any information that foreign governments provide to NSA as a result of such technical or linguistic assistance may be disseminated by NSA in accordance with these minimization procedures. ~~(S)~~

10-31-11
Date

Eric H. Holder, Jr.
Attorney General of the United States

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
DAVID GREENE (SBN 160107)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
BENJAMIN W. BERKOWITZ (SBN 244441)
JUSTINA K. SESSIONS (SBN 270914)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700
Fax: (650) 813-9777

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **PLAINTIFFS' REPLY Re QUESTION THREE (*Clapper*) OF THE COURT'S FOUR QUESTIONS** **Hearing Date Not Yet Set** Courtroom 11, 19th Floor The Honorable Jeffrey S. White

EXHIBIT A

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE MOTION FOR DECLARATORY JUDGMENT OF A FIRST AMENDMENT RIGHT TO PUBLISH AGGREGATE INFORMATION ABOUT FISA ORDERS	)	Docket No. Misc. 13-03
IN RE MOTION TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS	)	Docket No. Misc. 13-04
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	)	Docket No. Misc. 13-05
IN RE MOTION FOR DECLARATORY JUDGMENT TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS AND DIRECTIVES	)	Docket No. Misc. 13-06
IN RE MOTION FOR DECLARATORY JUDGMENT TO REPORT AGGREGATED DATA REGARDING FISA ORDERS	)	Docket No. Misc. 13-07

NOTICE

The Government hereby informs the Court that, pursuant to the terms of the attached letter from the Deputy Attorney General, the Government will permit the petitioners to publish the aggregate data at issue in the above-captioned actions relating to any orders issued pursuant to the Foreign Intelligence Surveillance Act (FISA). The parties are separately stipulating to the

dismissal of these actions without prejudice. The Director of National Intelligence has declassified the aggregate data consistent with the terms of the attached letter from the Deputy Attorney General, in the exercise of the Director of National Intelligence's discretion pursuant to Executive Order 13526, § 3.1(c). The Government will therefore treat such disclosures as no longer prohibited under any legal provision that would otherwise prohibit the disclosure of classified data, including data relating to FISA surveillance. It is the Government's position that the terms outlined in the Deputy Attorney General's letter define the limits of permissible reporting for the parties and other similarly situated companies.

Dated: January 27, 2014

Respectfully submitted,

JOHN P. CARLIN
Acting Assistant Attorney General
for National Security

TASHINA GAUHAR
Deputy Assistant Attorney General
National Security Division

J. BRADFORD WIEGMANN
Deputy Assistant Attorney General
National Security Division

CHRISTOPHER HARDEE
Chief Counsel for Policy
National Security Division

/s/ Alex Iftimie
ALEX IFTIMIE
U.S. Department of Justice
National Security Division
950 Pennsylvania Ave., N.W.
Washington, DC 20530
Phone: (202) 514-5600
Fax: (202) 514-8053

Attorneys for the United States of America

CERTIFICATE OF SERVICE

I hereby certify that a true copy of this Notice was served by the Government via email on this 27th day of January, 2014, addressed to:

Albert Gidari
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
Attorney for Google Inc.

James Garland
David N. Fagan
Alexander A. Berengaut
Covington & Burling LLP
1201 Pennsylvania Avenue, N.W.
Washington, DC 20004-2401
Attorneys for Microsoft Corporation

Marc J. Zwillinger
Jacob A. Sommer
ZwillGen PLLC
1705 N Street, N.W.
Washington, DC 20036
Attorneys for Yahoo! Inc.

Carl J. Nichols
Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue, N.W.
Washington, DC 20006
Attorney for Facebook, Inc.

Jerome C. Roth
Jonathan H. Blavin
Justin P. Raphael
Munger, Tolles & Olson LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
Attorneys for LinkedIn Corporation

/s/
Alex Iftimie

Office of the Deputy Attorney General
Washington, D.C. 20530

January 27, 2014

Sent via Email

Colin Stretch, Esquire
Vice President and General Counsel
Facebook Corporate Office
1601 Willow Road
Menlo Park, CA 94025

Kent Walker, Esquire
Senior Vice President and General Counsel
Google Corporate Office Headquarters
1600 Amphitheater Parkway
Mountain View, CA 94043

Erika Rottenberg, Esquire
Vice President, General Counsel/Secretary
LinkedIn Corporation
2029 Stierlin Court
Mountain View, CA 94043

Brad Smith, Esquire
Executive Vice President and General Counsel
Microsoft Corporate Office Headquarters
One Microsoft Way
Redmond, WA 98052-7329

Ronald Bell, Esquire
General Counsel
Yahoo Inc. Corporate Office and Headquarters
701 First Avenue
Sunnyvale, CA 94089

Dear General Counsels:

Pursuant to my discussions with you over the last month, this letter memorializes the new and additional ways in which the government will permit your company to report data concerning requests for customer information. We are sending this in connection with the Notice we filed with the Foreign Intelligence Surveillance Court today.

In the summer of 2013, the government agreed that providers could report in aggregate the total number of all requests received for customer data, including all criminal process, NSLs,

and FISA orders, and the total number of accounts targeted by those requests, in bands of 1000. In the alternative, the provider could separately report precise numbers of criminal process received and number of accounts affected thereby, as well as the number of NSLs received and the number of accounts affected thereby in bands of 1000. Under this latter option, however, a provider could not include in its reporting any data about FISA process received.

The government is now providing two alternative ways in which companies may inform their customers about requests for data. Consistent with the President's direction in his speech on January 17, 2014, these new reporting methods enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

Option One.

A provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.

2. The number of NSLs received, reported in bands of 1000 starting with 0-999.

3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.

4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.

5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.

6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.[1]

7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered

[1] As the Director of National Intelligence stated on November 18, 2013, the Government several years ago discontinued a program under which it collected bulk internet metadata, and no longer issues FISA orders for such information in bulk. See http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence. With regard to the bulk collection of telephone metadata, the President has ordered a transition that will end the Section 215 bulk metadata program as it currently exists and has requested recommendations about how the program should be restructured. The result of that transition will determine the manner in which data about any continued collection of that kind is most appropriately reported.

by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.

In addition, there will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a "New Capability Order" because disclosing it would reveal that the platform, product, or service is subject to previously undisclosed collection through FISA orders. For example, a report published on July 1, 2015, will not reflect data relating to any New Capability Order received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017. After data about a New Capability Order has been published, that type of order will no longer be considered a New Capability Order, and the ordinary six-month delay will apply.

The two-year delay described above does not apply to a FISA order directed at an enhancement to or iteration of an existing, already publicly available platform, product, or service when the company has received previously disclosed FISA orders of the same type for that platform, product, or service.

A provider may include in its transparency report general qualifying language regarding the existence of this additional delay mechanism to ensure the accuracy of its reported data, to the effect that the transparency report may or may not include orders subject to such additional delay (but without specifically confirming or denying that it has received such new capability orders).

Option Two.

In the alternative, a provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.

2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.

3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

* * *

I have appreciated the opportunity to discuss these issues with you, and I am grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency. We look forward to continuing to discuss with you ways in which the

government and industry can similarly find common ground on other issues raised by the surveillance debates of recent months.

Sincerely,

James M. Cole
Deputy Attorney General

FOR THE NORTHERN DISTRICT OF CALIFORNIA

AMENDED CIVIL MINUTE ORDER

DATE: September 27, 2013 Time in Court: 31 minutes

JUDGE: JEFFREY S. WHITE Court Reporter: Debra Pas

Courtroom Deputy: Jennifer Ottolini

CASE NO. C-08-4373 and C-07-693 JSW

TITLE: Carolyn Jewel, et al., v. National Security Agency, et al.,
Virginia Shubert, et al., v. George W. Bush, et al.,

COUNSEL FOR PLAINTIFF:
Ilann Maazel
Cindy Cohn
Thomas Moore III
Richard Weibe
Benjamin Berkowitz

COUNSEL FOR DEFENDANT:
Anthony Coppolino
Jim Whitman

PROCEEDINGS: Status Conference

RESULTS: Status Conference held.

The Court set the following briefing schedules regarding outstanding FOIA issues discussed:

For Defendants:

- Opening briefs due: December 20, 2013
- Opposition briefs due: January 31, 2014
- Reply briefs due: February 28, 2014

For Plaintiffs:

- Opening briefs due: January 31, 2014
- Opposition briefs due: February 14, 2014
- Reply briefs due: February 28, 2014

A hearing will be schedule by further order of the Court.

Pursuant to the parties' stipulation, the Court STAYS the claims against the personal capacity Defendants and STAYS substitution of deceased Plaintiff Gregory Hicks, until further order of the Court, upon a showing of good cause.

Discovery shall not commence until resolution of the four threshold legal issues requiring further briefing.

- Defendants' revised declarations and exhibits due: December 20, 2013
- Plaintiffs' response, if any, due: January 10, 2014

The Court directed the parties to order a transcript of these proceedings.

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

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

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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. 08-CV-4373-JSW **DECLARATION OF RICHARD R. WIEBE IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' STAY REQUEST** Courtroom 11, 19th Floor The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action. I certify that the exhibit attached hereto is a true and correct copy of the document located at the indicated source.

2. As part of the FISA Amendments Act of 2008, Congress required the Inspectors General of the National Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President's Surveillance Program to investigate and report to Congress upon the Program. Section 301(b)(1) of the FISA Amendments Act of 2008 provides:

> "The Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President's Surveillance Program, shall complete a comprehensive review of, with respect to the oversight authority and responsibility of each such Inspector General—
>
> (A) all of the facts necessary to describe the establishment, implementation, product, and use of the product of the Program;
>
> (B) access to legal reviews of the Program and access to information about the Program;
>
> (C) communications with, and participation of, individuals and entities in the private sector related to the Program;
>
> (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and
>
> (E) any other matters identified by any such Inspector General that would enable that Inspector General to complete a review of the Program, with respect to such Department or element."

FISA Amendments Act of 2008, Pub. L. 110-261, § 301(b)(1), 122 Stat. 2436, 2471-2472 (2008).

3. Plaintiffs have previously submitted to the Court the unclassified joint report of the Inspectors General, which was released on July 10, 2009. Dkt. #35, Ex. A.

4. In addition to their joint report, each of the Inspectors General prepared an individual report describing his or her agency's participation in the President's Surveillance Program.

5. Attached hereto as **Exhibit A** is the March 24, 2009 "Working Draft" of the NSA Inspector General's individual report. Exhibit A was obtained from the website of the *Guardian* newspaper, which published it June 27, 2013: http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

6. Exhibit A states:

> "This report provides the classified results of the NSA Office of the Inspector General (OIG) review of the President's Surveillance Program (PSP) as mandated in the FISA Amendments Act (FAA) of 2008. It includes the facts necessary to describe from NSA's perspective:
>
> - establishment of the PSP (Section One)
> - implementation and product of the PSP (Section Two)
> - access to legal reviews of the PSP and access to information about the PSP (Section Three)
> - interaction with the Foreign Intelligence Surveillance Court (FISC) and transition to court orders related to the PSP (Section Four)
> - oversight of PSP activities at NSA (Section Five)"

Exhibit A at 1-2.

Exhibit A describes in detail all four aspects of the NSA's communications surveillance and collection program: Telephone metadata, telephone content, Internet metadata, and Internet content.

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

Executed at San Francisco, CA on July 2, 2013.

s/ *Richard R. Wiebe*
Richard R. Wiebe

EXHIBIT A, Part 1 of 5

ST-09-0002 WORKING DRAFT

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

24 March 2009

(U) TABLE OF CONTENTS

ST-09-0002 WORKING DRAFT

I. (U) INTRODUCTION

Background

(U//FOUO) On 4 October 2001, President George W. Bush issued a memorandum entitled "AUTHORIZATION FOR SPECIFIED ELECTRONIC SURVEILLANCE ACTIVITIES DURING A LIMITED PERIOD TO DETECT AND PREVENT ACTS OF TERRORISM WITHIN THE UNITED STATES." The memorandum was based on the President's determination that after the 11 September 2001 terrorist attacks in the United States, an extraordinary emergency existed for national defense purposes.

(TS//SI//OR/NF) The 4 October 2001 Presidential authorization delegated authority to the Secretary of Defense, who further delegated it to the Director of National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) to conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried into or out of the United States, it would otherwise have required FISC authority.

(TS//SI//OR/NF) The Authorization specified that NSA could acquire the content and associated metadata of telephony and Internet communications for which there was probable cause to believe that one of the communicants was in Afghanistan or that one communicant was engaged in or preparing for acts of international terrorism. In addition, NSA was authorized to acquire telephony and Internet metadata[1] for communications with at least one communicant outside the United States or for which no communicant was known to be a citizen of the United States. NSA was also allowed to retain, process, analyze and disseminate intelligence from the communications acquired under the authority. [2]

(U) This Report

(U//FOUO) This report provides the classified results of the NSA Office of the Inspector General (OIG) review of the President's Surveillance Program (PSP) as mandated in the FISA Amendments Act (FAA) of 2008. It includes the facts necessary to describe from NSA's perspective:

[1] (U)Metadata is data that describes content, events, or networks associated with SIGINT targets.
[2] (U)The Authority changed over time. See Appendix B for details.

ST-09-0002
WORKING DRAFT

- ☒ establishment of the PSP (Section One)
- ☒ implementation and product of the PSP (Section Two)
- ☒ access to legal reviews of the PSP and access to information about the PSP (Section Three)
- ☒ interaction with the Foreign Intelligence Surveillance Court (FISC) and transition to court orders related to the PSP (Section Four)
- ☒ oversight of PSP activities at NSA (Section Five)

(U) President's Surveillance Program Terminology

(U//FOUO) For purposes of this report, the PSP, or "the Program," refers to NSA activities conducted under the authority of the 4 October 2001 memorandum and subsequent renewals, hereafter known as "the Authorization." As mandated by the FAA, this review includes activities authorized by the President between 11 September 2001 and 17 January 2007 and those activities continued under FISC authority. This includes the program described by the President in a 17 December 2005 radio address as the Terrorist Surveillance Program, which was content collected under the Authorization.

WORKING DRAFT

(TS//SI//NF) Foreign selectors tasked for PSP content collection did not require formal approvals or tasking packages. Analysts were responsible for determining whether a foreign selector met the criteria for foreign intelligence ~~terms of the Authorization~~.

(TS//SI//NF) **Collection.** After a ~~domestic~~ selector was approved for PSP ~~content~~ collection, it was identified as "tasked" in the STELLARWIND Addresses Database by CT/AAD tasking managers who then emailed a collection tasking request to the SSO Collection Manager for telephony and Internet content collection. Foreign selector content collection requests were sent directly to the SSO Collection Manager. They did not require special approval.

(TS//SI//STLW//NF) SSO collection managers were responsible for ensuring that telephony and Internet content selectors were put on or taken off collection. For ~~telephony~~ telephony content selectors, collection managers sent content collection tasking instructions to private sector companies. Private sector companies were responsible for implementing tasking at front-end devices to obtain the required content collection. For Internet content selectors, collection managers sent content tasking instructions directly to equipment installed at company-controlled locations. Collected data was sent back to NSA/SSO and made available to analysts through the HYBRID voice processing system for telephony content selectors or the PINWALE database for Internet content selectors. SSO collection managers worked with private sector companies and the CT Product Line to ensure that collected data was as intended and legally authorized.

(TS//SI//NF) **Storage.** Content (voice or d~~D~~ata) collected under PSP was stored in protected partitions in existing NSA databases. Access to the partitions was restricted to PSP-cleared personnel.

(TS//SI//NF) **Reporting.** After analyzing content data collected under Presidential authority and identifying foreign intelligence information, counterterrorism analysts wrote reports. After an initial review within the CT Product Line, some reports were sent to SID Oversight and Compliance (O&C) for a second review for U.S. person identities. O&C reviewers determined whether the U.S. identities in the report were necessary to assess or understand the foreign intelligence information being reported or was required within the conduct of recipient's official duties. If an identity was found to be unnecessary, it was not reported. Before any U.S. person information was disseminated in reporting, internal NSA approvals were obtained as required by *United States Signals Intelligence Directive SP0018 – Legal Compliance and Minimization Procedures*.

WORKING DRAFT

(U) FOUR: NSA PRIVATE SECTOR RELATIONSHIPS

(TS//SI//NF) To conduct foreign intelligence-gathering activities under the PSP, NSA required the assistance of private companies, which provided access to international communications chokepoints in United States. Immediately after 11 September 2001, some private companies contacted NSA to offer support. Subsequent to PSP authorization, NSA sent request letters to companies stating that their assistance was authorized by the President with legal concurrence of the Attorney General.

(U) Need for Private Sector Cooperation

(TS//SI//NF) The United States carries out foreign intelligence activities through a variety of means. One of the most effective means is to partner with commercial entities to obtain access to information that would not otherwise be available.

(U//FOUO) Telephony

(TS//SI//NF) Most international telephone calls are routed through a small number of switches or "chokepoints" in the international telephone switching system en route to their final destination. The United States is a major crossroads for international switched telephone traffic. For example, in 2003, circuit switches worldwide carried approximately 180 billion minutes of telephone communications. Twenty percent of this amount, over 37 billion minutes, either originated or terminated in the United States, and another thirteen percent, over 23 billion minutes, transited the United States (neither originating nor terminating here). [NSA is authorized under Executive Order 12333 to acquire transiting telephone calls.]

(TS//SI//NF) NSA determined that under the Authorization it could gain access to approximately 81% of the international calls into and out of the United States through three corporate partners: COMPANY A had access to 39%, COMPANY B 28%, and COMPANY C 14%. NSA did not seek assistance from local exchange carriers, because that would have given NSA access primarily to domestic calls.

ST-09-0002
WORKING DRAFT

(U//FOUO) Internet Communications

(TS//SI//NF) Al Qaeda and associated terrorist organizations have made extensive use of the Internet. It is their preferred method of communication. Terrorists use Internet communications, particularly web-based services, because they are ubiquitous, anonymous, and usually free of charge. They can access Web-based email accounts and similar services from any origination point around the world.

(TS//SI//NF) The United States is a major Internet communications hub. The industry standard for characterization of the volume of Internet communications is bandwidth, which measures the amount of digital data transmitted in one second – bits per second or bps. For example, data available from 2002 shows that at that time, worldwide international bandwidth was slightly more than 290 Gbps[7]. Of that total, less than 2.5 Gbps was between two regions that did not include the United States.

(TS//SI//NF) The United States is also home to computer servers providing Internet communications services often used by terrorists. The majority of known terrorist email addresses that NSA has tracked are hosted on U.S.-based providers or foreign-managed providers hosted on servers in the United States. (e.g., [redacted].

(U//FOUO) Evolution of NSA Partnerships with Private Sector

(U) History of NSA Partnerships with Private Sector

(TS//SI//NF) As far back as World War II, NSA has had classified relationships with carefully vetted U.S. companies that assist with essential foreign intelligence-gathering activities. NSA maintains relationships with over 100 U.S. companies. Without their cooperation, NSA would not be able respond to intelligence requirements on a variety of topics important to the United States.

(TS//SI//NF) Two of the most productive SIGINT collection partnerships that NSA has with the private sector are with COMPANY A and COMPANY B. These two relationships enable NSA to access large volumes of foreign-to-foreign communications transiting the United States

[7](U) Gpbs is an abbreviation for Gigabits per second, which can also be described as one billion bits per second or 1,000,000,000 bps.

WORKING DRAFT

through fiber-optic cables, gateway switches, and data networks. They also provide foreign intelligence authorized under the FISA.

(TS//SI//NF) According to General Alexander, General Hayden's replacement as Director of NSA/CSS, if the relationships with these companies were ever terminated, the U.S. SIGINT system would be irrevocably damaged, because NSA would have sacrificed America's home field advantage as the primary hub for worldwide telecommunications.

(U) Partnerships after 11 September 2001

(TS//SI//NF) According to the former Deputy Chief of SSO, between 11 September 2001 and the 4 October 2001 Authorization, COMPANY A and COMPANY B contacted NSA and asked "what can we do to help?" COMPANY B personnel approached NSA SSO personnel through an existing program. They said they noticed odd patterns in domestic calling records surrounding the events of 11 September and offered call records and analysis. With no appropriate authority under which to accept the call records, NSA suggested the company contact the FBI.

(U//FOUO) Partnerships Supporting the PSP

(TS//SI//NF) Once the Authorization was signed on 4 October 2001, NSA began a process of identifying and visiting commercial entities requesting their support. While requesting help from corporate entities to support the PSP, NSA personnel made it clear that the PSP was a cooperative program and participation was voluntary. NSA knew that the PSP was an extraordinary program and understood if companies viewed it as too much of a liability.

(TS//SI//NF) NSA Approaches to Private Sector Companies

(TS//SI//NF) **2001:** On Columbus Day, 8 October 2001, NSA Special Source Operations (SSO) personnel responsible for the access relationships with corporate partners COMPANY A, COMPANY B, and COMPANY C were called in to work and informed that the President had authorized the PSP on 4 October 2001. The SSO personnel were tasked with initiating a dialog with the respective TS/SCI-cleared officials from COMPANIES A, B, and C to seek their cooperation under the new Authorization. Over the next few business days, SSO personnel met separately with officials from the three companies. Each company agreed to cooperate.

WORKING DRAFT

(TS//SI-ECI//NF) Letters for COMPANIES A, B, C, and E were couriered to the companies' local facility. COMPANY B sometimes picked up its letters at NSA Headquarters. Letters for COMPANY D were stored at NSA since no one at the company had the proper clearance to store them.

(U//FOUO) PSP Authorized Support to NSA

(TS//SI-ECI//NF) Private sector companies provided assistance to NSA under the PSP in three categories: telephone and Internet Protocol content, Metadata from Call Detail Records, and Internet Protocol Metadata.

(TS//ECI//NF) The PSP allowed content to be collected if the selected communication was one-end foreign or the location of the communicants could not be determined. Selectors (email addresses and telephone numbers) were provided by NSA's Office of Counterterrorism.

(TS//SI-ECI//NF) **Content: Telephony.** Under the PSP, companies provided the content of one-end-foreign international telephone calls (telephony content) and the content of electronic communications (email content) of al Qaeda and its affiliates. COMPANIES A, B, and C provided telephony content from communications links they owned and operated. They had been providing telephony content to NSA before 2001 under FISA and E.O. 12333 authorities. NSA began to receive telephony content from COMPANIES A and B on 6 October 2001 and COMPANY C on 7 October 2001. This support ended on 17 January 2007.

(TS//SI-ECI//NF) **Content: Internet Email**. COMPANIES A, B, and C provided access to the content of Al Qaeda and Al Qaeda-affiliate email from communication links they owned and operated. NSA received email content from COMPANY A as early as October 2001 until 17 January 2007, from Company B beginning February-March 2002 through 17 January 2007, and from COMPANY C from April 2005 until 17 January 2007. From April 2003 through November 2003, COMPANY D provided a limited amount of email content under the PSP. It did not provide PSP-related support after November 2003, but it did provide support under FISA.

(TS//SI-ECI//NF) **Metadata from Call Detail Records**. COMPANIES A and B provided Call Detail Records to NSA. The records were used by NSA Counter-Terrorism metadata analysts to perform call chaining and network reconstruction between known al Qaeda and al Qaeda-affiliate telephone numbers and previously unknown telephone numbers with which they had been in contact. Providers generated Call Detail Records as a normal course of doing business (e.g., billing purposes and traffic

CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all other similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No. CV-08-4373-JSW

DECLARATION OF CINDY COHN PURSUANT TO FED. R. CIV. P. 56(d) IN OPPOSITION TO GOVERNMENT DEFENDANTS' MOTION TO DISMISS AND FOR SUMMARY JUDGMENT

Date: December 14, 2012
Time: 9:00a.m.
Dept: 11, 19th Floor
Judge: Jeffrey S. White

I, CINDY COHN, declare and state:

1. I am an attorney duly licensed to practice law in the courts of the State of California, and I am a member of the bar of this district. I am also Legal Director for the Electronic Frontier Foundation, counsel of record to the Plaintiffs in this action. I am familiar with the records and proceedings in this action.

2. The Government here has not filed an answer to the complaint in this case, and discovery has not begun. However, because the Government has styled its motion as a motion to dismiss or alternatively for summary judgment, Plaintiffs are compelled to invoke their rights under Rule 56(d) to have an opportunity to conduct discovery to obtain "facts essential to justify its opposition" to summary judgment.

3. Along with this opposition, Plaintiffs are filing an extensive factual record that establishes the genuine issues as to the material facts surrounding the Government's unlawful surveillance of millions of ordinary Americans. This Court may take judicial notice of the existence of that factual record under Federal Rule of Evidence 201. Plaintiffs summarize that factual record in their Summary of Voluminous Evidence filed under Federal Rule of Evidence 1006, also filed herewith.

4. In addition to the evidence Plaintiffs present herewith, Plaintiffs are entitled under Rule 56(d) to conduct discovery before the Court decides the Government's motion. Plaintiffs respectfully submit that further information supporting their opposition is in the hands of other parties and witnesses, including the Government and its agents and employees and the telecommunications companies and their agents and employees. Plaintiffs also submit that, while some of it may be classified, much of it is not. This is based on the ongoing series of government admissions to date documented in the evidence filed herewith, as well as information from whistleblowers, including former NSA employees, members of Congress and other information that is not properly subject to any classification or other secrecy. Discovery is likely to reveal additional facts that will help demonstrate that there are genuine issues of material fact that preclude granting the Government's motion.

5. Similar to what the Court ordered in *Al-Haramain* (MDL Docket No. 537, page 23, lines 17-26), if necessary, at least some of Plaintiffs' attorneys would seek a security clearance in order to allow them to conduct discovery that may require such clearance in order to protect national security.[1]

6. The evidence that Plaintiffs intend to uncover through discovery is available through several channels, as outlined below.

7. Plaintiffs would take the deposition of former government officials who have spoken publicly about the communications carriers' involvement in the NSA's warrantless surveillance, including Defendants Richard B. Cheney, Michael B. Mukasey, John M. McConnell, David S. Addington, Alberto R. Gonzales, John D. Ashcroft, John D. Negroponte, Jack Goldsmith, John Yoo and nonparties Michael Chertoff, Keith B. Alexander, Michael V. Hayden, James Comey, Andrew Card, Patrick Philbin, Robert S. Mueller III, Thomas M. Tamm and Russell Tice. As noted above, if needed Plaintiffs would seek a security clearance to enable them to conduct this discovery in a manner that protects national security.

8. Plaintiffs would seek further written and deposition discovery arising out of the documents summarized in the accompanying Summary of Voluminous Evidence both to further develop any facts raised by them and to address any claims that any of the information in those documents requires authentication, is hearsay, or is otherwise inadmissible.

9. For instance, the Summary of Voluminous Evidence references the unclassified nature of 17 paragraphs of notes of then White House Counsel Alberto Gonzales' March 10, 2004 meeting with certain members of Congress known as the "Gang of Eight." The notes discuss legal concerns about the program. As the Inspector General of the Department of Justice reported: "The NSA officials determined that 3 of 21 paragraphs in the notes contains SCI

[1] The *Al-Haramain* Order stated in pertinent part:

> Unless counsel for plaintiffs are granted access to the court's rulings and, possibly, to at least some of defendants' classified filings, however, the entire remaining course of this litigation will be ex parte. This outcome would deprive plaintiffs of due process to an extent inconsistent with Congress's purpose in enacting FISA's sections 1806(f) and 1810. Accordingly, this order provides for members of plaintiffs' litigation team to obtain the security clearances necessary to be able to litigate the case, including, but not limited to, reading and responding to the court's future orders.

information about the NSA surveillance program [and] 1 paragraph contains SCI information about signals intelligence." Summary of Evidence at 36 (citing Office of the Inspector General, *U.S. Dept. of Justice, Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Att'y Gen. Alberto Gonzales* (Sep. 2, 2008), at p. 10, n.14). Those notes themselves are evidence, or at a minimum are likely to lead to the discovery of admissible evidence, about the scope and legal justification for some portion of the alleged surveillance.

10. Similarly, testimony regarding issues discussed at the March 10, 2004 meeting in Attorney General Ashcroft's hospital room is not classified, since non-cleared personnel were present. Summary of Evidence at 53 (citing *Oversight of the Department of Justice*: Hearing before the S. Comm. on the Judiciary, 110th Cong. at 67 (July 24, 2007)). Again, those issues are either directly relevant to the surveillance alleged in this case or are likely to lead to the discovery of admissible evidence about the facts of the surveillance that led to legal concerns about it at the Department of Justice.

11. Plaintiffs would take depositions of and seek documents from the named sources in the published reports filed herewith and described in the Summary of Voluminous Evidence, regarding those sources' personal knowledge of published or unpublished information or their discussions with or knowledge of other sources of information.

12. To the extent Plaintiffs are able independently to identify any additional sources of evidence, Plaintiffs would seek to obtain declarations from, or propound depositions on written questions to, any unnamed sources, including those quoted in news reports.

13. Plaintiffs would seek discovery regarding the fact of the carriers' interception and disclosure of the communications and communications records of the telecommunications companies' customers, including those of the named Plaintiffs and class members.

14. Plaintiffs would take the depositions of Qwest executives including Joseph Nacchio regarding non-privileged discussions with the NSA pertaining to warrantless wiretapping, including content data acquisition. Published accounts note that unlike AT&T, Qwest publicly disclosed that it received a request from the NSA to intercept and disclose customer communications and data, and that it rejected the request.

15. Plaintiffs would request an inspection of the premises of AT&T's Folsom Street facility under Fed. R. Civ. P. 34, including the WorldNet Internet room, the splitter cable, the inside and outside of the splitter cabinet, and the area outside the SG3 Secure Room. Plaintiffs would also request an inspection of the premises outside of other of AT&T's SG3 rooms, which the record indicates exist in Atlanta, Seattle, San Jose, San Diego, and Los Angeles. Declaration of Mark Klein ¶ 36 (Dkt. #85).

16. Plaintiffs would take the depositions (or obtain the sworn declarations) of current or former AT&T employees with knowledge of, and who worked in, the SG3 Secure Room, doing so in a manner that would protect the identities of these witnesses, as needed. Such persons would include, but are not limited to: (1) James W. Russell, who filed a Declaration dated April 10, 2006, under seal due to AT&T trade secret concerns, and (2) the named author of certain exhibits to the Klein Declaration that were also filed under seal.

17. Plaintiffs would seek third-party discovery about the network infrastructure of AT&T in order to confirm how Internet traffic is routed within its network and through fiber optic splitters in the facility on Folsom Street in San Francisco other AT&T facilities in order to confirm that all or nearly all of AT&T's customers are members of the class.

18. Plaintiffs would request an inspection of AT&T's facilities housing the Daytona database and databases used for similar purposes at AT&T and other carriers.

19. Plaintiffs would take depositions of the persons most knowledgeable about AT&T's Daytona database and databases used for similar purposes at AT&T and other carriers.

20. Each of the topics of specific discovery outlined above is highly likely to yield further evidence of genuinely disputed material facts relating to all of Plaintiffs' claims. Specifically, the discovery would lead to evidence regarding the nature and scope of the Government's surveillance program, the timing and substance of efforts to concoct a legal justification for the program, the nonexistence of judicial or other legal authority for the surveillance, the efforts to mislead Congress, the public and the FISA court about the illegal aspects of the program, and the intention on the part of the individual defendants to violate the Wiretap Act, SCA, FISA and the Fourth Amendment.

21. The discovery would confirm that many, if not all, of the salient points necessary for Plaintiffs to prove their claims are available through non-secret evidence that can be found through regular discovery processes.

22. Moreover, the discovery will confirm that Plaintiffs can prove their case even if the government is correct in its assertion that the state secrets privilege applies instead of the statutory provisions of 50 U.S.C. §1806(f). This is because, even if the government is correct on that point, the effect is that "[T]he privileged information is excluded and the trial goes on without it" (*General Dynamics*, 131 S. Ct. at 1906), "'with no consequences save those resulting from the loss of evidence.'" *Mohamed*, 614 F.3d at 1082; *see also Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007) ("[t]he effect of the government's successful invocation of privilege 'is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly'").

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

Executed at San Francisco, California, this 9th day of October 2012.

/s/ Cindy Cohn
CINDY COHN

CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
KURT OPSAHL (191303)
JAMES S. TYRE (083117)
MARK RUMOLD (279060)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

CASE NO. 08-CV-4373-JSW

DECLARATION OF J. SCOTT MARCUS FILED IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

(ORIGINALLY FILED IN THE RELATED CASE OF HEPTING v. AT&T, NO. 06-CV-0676)

Date: November 2, 2012
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action and plaintiffs in the related action of *Hepting, et al. v. AT&T Corp., et al.*, N.D. Cal. No. 06-CV-0672. I have personal knowledge of the facts set forth below, except as may be otherwise noted, and if called as a witness I could and would testify competently to them.

2. Attached hereto is the Declaration of J. Scott Marcus and accompanying exhibits, originally filed in the related *Hepting* action. Although portions of the Marcus Declaration and certain accompanying exhibits originally were filed under seal (*Hepting* Dkt. #130; #231; #277; #294), the entire Marcus Declaration and all exhibits were unsealed pursuant to stipulation and court order (*Hepting* Dkt. #294; #358 & Exs. 2, 3; #361). There is no confidential information in the Marcus Declaration or the accompanying exhibits.

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

Executed at San Francisco, CA on June 29, 2012.

s/ Richard R. Wiebe

Richard R. Wiebe

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
tien@eff.org
KURT OPSAHL (191303)
kurt@eff.org
KEVIN S. BANKSTON (217026)
bankston@eff.org
CORYNNE MCSHERRY (221504)
corynne@eff.org
JAMES S. TYRE (083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

TRABER & VOORHEES
BERT VOORHEES (137623)
bv@tvlegal.com
THERESA M. TRABER (116305)
tmt@tvlegal.com
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103
Telephone: 626/585-9611
626/ 577-7079 (fax)

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE (121156)
wiebe@pacbell.net
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200
415/433-6382 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN, on Behalf of Themselves and All Others Similarly Situated,,

Plaintiffs,

v.

AT&T CORP., et al.,

Defendants.

No. C-06-0672-VRW

CLASS ACTION

DECLARATION OF J. SCOTT MARCUS IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION

Date: June 8, 2006
Courtroom: 6, 17th Floor
Judge: Hon. Vaughn Walker

FILED UNDER SEAL PURSUANT TO CIVIL LOCAL RULE 79-5

LIST OF EXHIBITS

A	Curriculum vitae of J. Scott Marcus
B	Eric Lichtblau and James Risen, Spy Agency Mined Vast Data Trove, Officials Report, The New York Times, Dec. 24, 2005
C	Barton Gellman, Dafna Linzer and Carol D. Leonnig, Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared, Washington Post, Feb. 5, 2006
D	Marcus et al, "Internet interconnection and the off-net-cost pricing principle"
E	Marcus, "Call Termination Fees: The U.S. in global perspective"
F	Marcus, "What Rules for IP-enabled NGNs?"
G	"Evolving Core Capabilities of the Internet"
H	http://en.wikipedia.org/wiki/Modulation
I	http://en.wikipedia.org/wiki/Attenuation
J	http://en.wikipedia.org/wiki/Decibel
K	ADC brochure (Value-Added Module System: LGX Compatible)
L	http://www.narus.com/solutions/IPanalysis.html
M	http://www.ist-scampi.org/events/workshop-2004/poell.pdf
N	http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf
O	http://www.narus.com/platform/index.html
P	http://www.narus.com/solutions/NarusForensics.html
Q	In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges, FCC WC Docket 02-361, Petition of AT&T
R	Report of the NRIC V Interoperability Focus Group, "Service Provider Interconnection for Internet Protocol Best Effort Service"
S	Ch. 14, Marcus, Designing Wide Area Networks and Internetworks: A Practical Guide (1999)
T	http://www.broadbandweek.com/newsdirect/0208/direct020802.htm, August 2, 2002
U	http://www.narus.com/solutions/IPsecurity.html
V	http://www.fcw.com/article90916-09-26-05-Print
W	http://www.att.com/news/2004/03/22-12972

X http://www.eweek.com/print_article2/0,1217,a=139716,00.asp

Y Lehman Brothers analysis of AT&T (Jan. 24, 2003)

I, J. Scott Marcus, declare under the penalty of perjury that the following is true and correct:

1. The Electronic Frontier Foundation (EFF) has asked me to render an expert opinion[1] on the implications of a declaration by Mark Klein ("Klein Declaration"), and on a series of documents alleged to have been generated by AT&T (Exhibits A, B and C to the Klein Declaration) ("Klein Exhibits"), in conjunction with Plaintiffs' Motion for a Preliminary Injunction.

2. I am strongly of the opinion that the Klein Exhibits are authentic, and I find Mr. Klein's declaration to be fully consistent with the documents and entirely plausible.

3. The EFF specifically requested that I assess whether the program described in the Klein Declaration and Klein Exhibits is consistent with media reports about a program authorized by the President of the United States, under which the National Security Agency ("NSA") engages in warrantless surveillance of communications of people inside the United States ("the Program").

4. I was asked to review the following two news articles: Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, The New York Times, Dec. 24, 2005 (attached as Exhibit B), and Barton Gellman, Dafna Linzer and Carol D. Leonnig, *Surveillance Net Yields Few Suspects: NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, Washington Post, Feb. 5, 2006 at A01 (attached as Exhibit C).

5. I was asked to focus on the following claims in these two news articles, with respect to AT&T Corp.: that major U.S. telecommunications companies are assisting the government in carrying out the Program; that these companies have given the government direct access to telecommunications facilities physically located on U.S. soil; that by virtue of this access, the government can now monitor both domestic and international communications of persons in the United States; and that surveillance under the Program is conducted in several stages, with the early stages being computer-controlled collection and analysis of communications and the last stage being actual human scrutiny.

6. In the sections that follow, I present my qualifications, and provide an overview of

[1] Attached hereto as Exhibit A is my curriculum vitae.

the implications of the Klein Declaration and Klein Exhibits. I present my conclusions in regard to the scope of the program, and the volume of data that was captured. I also explain why I find credible Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale.

QUALIFICATIONS

7. For more than 30 years, I have worked in a wide range of positions involving computers, data communications, economics, and public policy. This declaration draws on my experience in several of these positions, and in several different academic disciplines.

8. From March 1990 to July 2001, I held a series of responsible positions with Bolt, Beranek and Newman (which was renamed BBN Corp.) and with its successor companies, GTE Internetworking and Genuity, culminating in my work as Chief Technology Officer (CTO) of Genuity.

9. BBN Corp. was acquired by GTE Corp. in 1997. The portion of BBN that functioned as an Internet Service Provider (ISP)[2] became GTE Internetworking, a wholly owned subsidiary of GTE.

10. In 2000, at the time of the Bell Atlantic – GTE merger (which formed Verizon), GTE Internetworking was spun out into an independent company in order to satisfy regulatory obligations relevant to the merger. The independent firm was called Genuity.

11. My primary engineering competence is as a designer of large scale IP-based[3] data networks.

12. Immediately following BBN's acquisition by GTE, I headed the team of systems architects and network engineers who developed the overall architectural design for GTE Internetworking's new data network. The team, comprising of as many as 50 senior engineers at various times, translated general business and marketing requirements into a comprehensive set of

---

[2] An *Internet Service Provider (ISP)* is an organization that enables other organizations to connect to the global Internet. ISPs often provide additional supporting services to enable electronic mail (e-mail) and to permit domain names (such as www.fcc.gov) to be recognized.

[3] All Internet traffic is *IP-based*, *i.e.* based on the Internet Protocol. I expand on this discussion in the section in which I discuss "Traffic captured".

high level engineering designs. This was a project of substantial scope and scale. The new network transformed 13,000 miles of dark fiber[4] into a single integrated network providing nationwide (and ultimately global) high speed Internet access services, and support for consumer Internet access via broadband and dial-up, and high speed data services for large enterprises. In terms both of scope and of technology, this network was at the state of the art of the day. The network was viewed as a technical and economic success, and became in short order one of the largest Internet backbone networks in the world – in terms of traffic carried, it could be viewed as the fourth largest Internet *backbone*[5] in the world for much of the time that I was there.

13. I have some experience with AT&T's network at its inception. When AT&T initially entered the Internet business in 1995, they contracted with my firm, BBN, to provide the underlying service. In effect, they "private labeled" a BBN service. They provided connections to their customers over dedicated circuits, which were cross-connected to BBN's Internet network. The customer perceived an AT&T-branded service, but BBN provided the acual ISP services. I was BBN's lead technical person for this endeavor.

14. BBN and AT&T conducted exploratory, but ultimately unsuccessful, discussions about building an Internet backbone together. AT&T ultimately decided to implement their own Internet backbone network (the Common Backbone [CBB],[6] which is the same name used in these documents), and thus to assume the ISP functions that had previously been provided by BBN. The initial design of the CBB reflected AT&T's experience in working with BBN.

15. In addition to the GTE Internetworking's own Internet backbone, and the work with AT&T, I designed a number of networks for commercial and government customers. I did the initial design work and cost analysis for a very large dial-up network for America Online in 1995.

---

[4] Fiber optics are discussed later in this declaration. Dark fiber is fiber optic cable that is not yet carrying traffic.

[5] The term *backbone* is widely used in the industry, but not precisely defined. An Internet backbone can be thought of as a large ISP, many of whose customers may themselves be smaller ISPs. There is no single network that is *the Internet*; rather, the Internet backbones collectively form the core of the global Internet. The term backbone is also sometimes used to denote any large IP-based network, whether used to provide IP-based services to the public or not.

[6] The AT&T Common Backbone, like backbones generally, is a large IP-based network. The CBB is used for the transmission of interstate or foreign communications.

This network ultimately carried as much as 40% of America Online's dial-up traffic.

16. My experience as CTO at GTE Internetworking provides useful insights not only in network design, but also into operational procedures in a large Internet backbone operator associated with a large traditional telecommunications carrier. BBN's joint project with AT&T required me to work closely with AT&T's engineers as they deployed the service. In addition, much of BBN's Internet equipment was physically deployed into points of presence owned and operated by WorldCom and by MCI, which required that I be able to coordinate with their staffs as well. These insights into carrier operations enable me to assess the AT&T documents.

17. Many of my other duties at BBN, GTE Internetworking and Genuity are relevant to this declaration.

18. I created a network design and capacity planning function within BBN, and ran the function for several years. In the context of an ISP, capacity planning is the process whereby the ISP measures and interprets current service demands on the network, projects future demands (considering both current and projected future service offerings), and plans for necessary network enhancements to meet those demands. Capacity planning required constant interaction with the company's financial planners, as well as marketing and engineering. It also required an in-depth understanding of traffic flows within and between Internet providers. After the merger with GTE, I received a GTE Chairman's Leadership Award for that work.

19. I am the author of a textbook on data network design: *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999. The book largely reflects my experience with capacity planning and network design in the large at BBN, GTE Internetworking and Genuity.

20. I held a number of sales and marketing positions at BBN, and in those roles (and also subsequently as Genuity's CTO) frequently participated in the assessment of the costs and the potential revenues associated with new services.

21. Many of my outside consulting assignments at BBN involved elements of data security and network security. Later, as CTO, the company's senior security expert was a direct report. I thus had a general oversight role with respect to the company's performance of lawful

intercept.

22. As CTO, I also had primary responsibility for the company's strategic approach to peering[7] with other Internet Service Providers (including AT&T). I personally chaired the firm's peering policy council, where the company's various stakeholders (engineering, financial and marketing) established strategic direction in regard to peering.

23. I supported GTE's General Counsel in raising concerns about the MCI-WorldCom merger (1998) and the proposed MCI-Sprint merger (2000), arguing that the network externality effects resulting from the mergers would make anticompetitive practices as regards Internet backbone peering both feasible and profitable. These arguments hinged to a substantial degree on my ability to estimate peering traffic flows between the major Internet backbones in both real and hypothetical circumstances. This activity drew heavily on my experience with the measurement and analysis of traffic.

24. From July 2001 to July 2005, I was the Senior Advisor for Internet Technology at the Federal Communications Commission (FCC). In this role, I served as the FCC's leading technical expert on the Internet, and provided advice to the Chairman's office and to other senior managers as regards technology and policy issues.

25. I participated in numerous proceedings during my time at the FCC, including several that dealt generally with broadband and with Voice over IP (VoIP).[8]

26. I was a member of the FCC's Homeland Security Policy Council, with significant responsibilities as regards cybersecurity and infrastructure security. I held a top secret clearance. I frequently spoke on the FCC's behalf on lawful intercept (CALEA)[9] in connection with IP-based services. I was an active and significant participant in the FCC's proceedings related to CALEA in

---

[7] *Peering* is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. A more extensive definition appears later in this Declaration, under "Traffic Captured."

[8] *IP* is the Internet Protocol. All Internet data is IP-based. *Voice over IP* refers to the transmission of voice over IP-based networks – either private networks or the "public" Internet.

[9] Communications Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279. CALEA is the statute that requires carriers to proactively instrument their networks in order to support law enforcement needs. The FCC has a role in its implementation.

connection with Voice over IP (VoIP) and with broadband.

27. From July 2005 to the present, I have been a Senior Consultant for the WIK, located in Bad Honnef, Germany. The WIK is a leading German research institute specializing in the economics of electronic communications, and the regulatory implications that flow from those economics. Much of my current work applies economic reasoning to policy problems in electronic communications.

28. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and have held several senior volunteer positions within the IEEE. I am currently co-editor for public policy and regulatory matters for *IEEE Communications Magazine*. I have also served as a trustee of the American Registry of Internet Numbers (ARIN).

29. I do not consider myself an economist, but I have a good working knowledge of economics as it applies to the aspects of telecommunications that I deal with. Several of my professional papers over the past few years are economics papers, and a number of them have been cited by recognized economists.[10] Other recent papers apply economic reasoning to problems in the regulation of electronic communications.[11]

BACKGROUND –DOCUMENTS REVIEWED

30. In forming my expert opinions in this Declaration, I reviewed the following documents: the Klein Declaration; *SIMS Splitter Cut-In and Test Procedure*, Issue 2, 01/13/03

---

[10] See, for instance, my paper with Jean-Jacques Laffont, Patrick Rey, and Jean Tirole, IDE-I, Toulouse, "Internet interconnection and the off-net-cost pricing principle," *RAND Journal of Economics*, Vol. 34, No. 2, Summer 2003, available at http://www.rje.org/abstracts/abstracts/2003/rje.sum03.Laffont.pdf (Exhibit D). An earlier version of the paper appeared as "Internet Peering," *American Economics Review*, Volume 91, Number 2, May 2001. See also "Call Termination Fees: The U.S. in global perspective," presented at the 4th ZEW Conference on the Economics of Information and Communication Technologies, Mannheim, Germany, July 2004, available at: ftp://ftp.zew.de/pub/zew-docs/div/IKT04/Paper_Marcus_Parallel_Session.pdf (Exhibit E). Another paper that deals primarily with economics has been commissioned by the International Telecommunications Union (ITU-T) for presentation at their ITU New Initiatives Workshop on "What Rules for IP-enabled NGNs?," March 23-24, 2006: "Interconnection in an NGN environment," available at http://www.itu.int/osg/spu/ngn/documents/Papers/Marcus-060323-Fin-v2.1.pdf (Exhibit F).

[11] *See*, for instance, "Evolving Core Capabilities of the Internet," *Journal on Telecommunications and High Technology Law*, 2004 (Exhibit G).

(Klein Decl. Exh. A); *SIMS Splitter Cut-In and Test Procedure: OSWF Training*, Issue 2, January 24, 2003 (Klein Decl. Exh. B); and *Study Group 3 LGX/Splitter Wiring: San Francisco*, Issue 1, 12/10/02 (Klein Decl. Exh. C).

31. I have also reviewed publicly available data on the Internet – wherever I have relied on such data, I have so indicated in the text.

32. The Klein Exhibits use terms such as "SG3 equipment" and "SG3 room." I believe *SG3* to be an acronym for *Study Group 3*, which is used consistently to describe the project. Consistent with this terminology, I will refer to the *SG3 Configuration* throughout this declaration.

33. I interpret *OSWF* as a reference to the *On Site Work Force*. These documents represent directions to technicians who must "cut" the new facilities into the network, *i.e.* install them with as little impact as possible on AT&T's ongoing network operations.

34. Based on my experience in working with AT&T, I consider the documents to be written with the meticulous attention to detail that is typical of AT&T operations. Highly skilled central engineering staff provided unambiguous and highly detailed directions in order to enable implementation by multiple on site field crews at a lower skill level. Any operations that could be done in advance were dealt with prior to the cut. The cut was designed to be as fast and as painless as possible, so as to minimize the risk of network disruption. The cut was to take place during the maintenance window (presumably during the early morning hours, *e.g.* 2:00 AM) so as to further minimize possible disruption.[12]

35. It is clear that these plans relate to real deployments, and not just to a theoretical or hypothetical exercise. The last page of Klein Exhibit B makes clear that the San Francisco deployment was already in full swing when the document was published on January 24, 2003. Of sixteen large peering circuits that were to be diverted, (1) circuit engineering was complete for eight, (2) actual change orders had already been issued for four, and were scheduled to be issued for four more within the subsequent week (i.e. by 1/30/2003), and (3) request dates had been established for the completion of the remaining circuit engineering, for splitter pre-test and for

[12] *See* Klein Exh. A, page 4.

putting the splitters into the circuits, all in 1/2003 and 2/2003.

36. Klein Exhibit B and Klein Exhibit C are specific to AT&T's San Francisco facility, but Klein Exhibit A is generic – it is relevant to all sites where this cut was to take place.

OVERVIEW AND SUMMARY OF PRINCIPAL OPINIONS

37. My expert assessment is based on the Klein Declaration, the AT&T documents collectively designated as the Klein Exhibits, my extensive and varied experience in the industry, and various publicly available documents. Where I have relied on such documents, I have so indicated in the text.

38. Based on these documents, other publicly available documents, and my general knowledge of the industry, I conclude that AT&T has constructed an extensive – and expensive – collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well.*[13]

39. In terms of the media claims I was asked to evaluate with respect to AT&T, I conclude that: the infrastructure described by the Klein Declaration and Klein Exhibits provides AT&T Corp. with the capacity to assist the government in carrying out the Program; that the infrastructure deployed included a data network (the *SG3 backbone*) that apparently provided third party access to the SG3 room or rooms; that, if the government is in fact in communication with this infrastructure, AT&T Corp. has given the government direct access to telecommunications facilities physically located on U.S. soil; that, by virtue of this access, the government would have the capacity to monitor both domestic and international communications of persons in the United States; and that surveillance under the Program is conducted in several stages, with the early stages being computer-controlled collection and analysis of communications and the last stage being actual human scrutiny.

40. A key question is whether the infrastructure that AT&T deployed – which I refer to for purposes of this declaration as the *SG3 Configurations* – is being used solely for legitimate or

[13] Later in this Declaration, I provide my assessment of the volume of domestic and international traffic captured.

innocuous purposes, or for interception that violates consumer privacy and U.S. law. The SG3 Configurations could be used for a number of legitimate purposes; however, the scale of these deployments is, in my opinion and based on my experience, vastly in excess of what would be needed for any likely application, or any likely combination of applications other than surveillance.

41. The SG3 Configurations that were deployed are not routine for Internet backbone operators, and they are emphatically not required (nor, apparently, are they being used) for the transmission of Internet data between customers.

42. I consider other possible alternative hypotheses for AT&T's deployments later in this Declaration, under "Alternative reasons why AT&T might have deployed the SG3 Configurations." For instance, the SG3 Configurations could be used in support of routine lawful intercept, and are possibly being used in that way, but lawful intercept requirements could not account for AT&T's deployment of the SG3 deployments. As another example, the SG3 Configurations could be used in support of AT&T commercial security offerings, and it appears that AT&T is using either the SG3 Configurations or, more likely, similar technology deployed elsewhere in support of their Internet Protect commercial offering. In my judgment, and based on my experience, it is highly unlikely that benign applications, either individually or collectively, provided the rationale for the deployment. The information at hand suggests, rather, that AT&T has attempted after the fact to find ways to realize additional commercial value out of a very substantial deployment that had already been made primarily in order to conduct (presumably warrantless) surveillance. Public statements by AT&T officials over the years tend to support this view – AT&T only belatedly realized that customers might be interested in certain of these capabilities.[14]

43. Prior to seeing the Klein Declaration, I would have expected the Program to involve a modest and limited deployment, targeted solely at overseas traffic, and likely limited in the information captured to traffic measures (except pursuant to a warrant). The majority of international IP traffic enters the United States at a limited number of locations, many of them in the areas of northern Virginia, Silicon Valley, New York, and (for Latin America) south Florida.

[14] Supporting detail appears later in this Declaration, in "Alternative reasons why AT&T might have deployed the SG3 Configurations."

This deployment, however, is neither modest nor limited, and it apparently involves considerably more locations than would be required to catch the majority of international traffic.

44. The SG3 Configurations are fully capable of pattern analysis, pattern matching and detailed analysis at the level of *content*, not just of addressing information. One key component, the NARUS 6400, exists primarily to conduct sophisticated rule-based analysis of content. It is also well suited to high speed data reduction – to the "winnowing down" of large volumes of data, in order to identify only events of interest.

45. Klein Exhibit C speaks of a private SG3 backbone network, which appears to be partitioned from AT&T's main Internet backbone, the CBB.[15] This suggests the presence of a private network. The most plausible inference is that this was a covert network that was used to ship data of interest to one or more central locations for still more intensive analysis. I return to the capabilities of the SG3 Configurations later in this Declaration, under "Capabilities of the SG3 Configuration."

46. Given the probable cost of these configurations, and the likely limited commercial return, I find it exceedingly unlikely a financially troubled AT&T[16] would have made these investments at that time on its own initiative. I can envision no commercial reason, nor any combination of commercial reasons, that would render that investment likely. I therefore conclude that it is highly probable that funding came from an outside source, and consider the U.S. Government to be the most likely source. This supports Mr. Klein's assertion that the room was an NSA secure room, accessible only to NSA-cleared personnel.

47. I also find that the components that were chosen are exceptionally well suited to a massive, distributed surveillance activity (*see* "Capabilities of the SG3 Configuration" later in this Declaration). No other application provides as good an explanation for the combination of engineering choices that were made.

48. In addition, the private SG3 backbone network referred to in Klein Exhibit C,

---

[15] Klein Exh.C, pp 6, 12, 42. Again, *see* "Capabilities of the SG3 Configuration" later in this Declaration.

[16] I return to the topic of AT&T's financial condition later in this Declaration, under "AT&T's Financial Condition in 2003."

appears to be partitioned from AT&T's main Internet backbone, the CBB.[17] This is perfectly consistent with the notion of massive, covert distributed surveillance system. It is not consistent with normal AT&T practice – they have been working for years to try to reduce the number of networks in use, in the interest of engineering and operational economy.

49. For all of these reasons, I am persuaded that the SG3 Configurations were deployed primarily in order to perform surveillance on a massive scale, and not for any other purpose.

BACKGROUND – FIBER OPTICS

50. The Klein Declaration speaks (at ¶ 24 and in the sections following) of *splitting* the light signal, so as to divert a portion of the signal to the SG3 Secure Room. It may be helpful to review (at an informal level suitable for a non-specialist) some of the characteristics of fiber optic transmission before proceeding.

51. Historically, electronic communications were carried over copper wires, or were broadcast through the air. In both instances, it was often economically and technically advantageous to *modulate*[18] the signal onto a higher frequency wave. Doing so enables the recipient to select from among multiple signals transmitted over the same physical medium. You do this every time that you tune your television or radio to a particular channel.

52. More recently, fiber optics have supplanted the use of copper wire for many applications, especially those involving long distances. Instead of modulating signals onto electrical waves or radio waves, they are modulated onto light waves. Because light waves have a much higher frequency than the waves used in copper wires, it is possible to modulate far more information onto them.

53. Fiber optics have an additional advantage over copper wires: They do not generate electrical interference, nor are they vulnerable to it. In addition, it is difficult to "tap" into a fiber

---

[17] Klein Exh.C, pp 6, 12, 42. Again, *see* "Capabilities of the SG3 Configuration" later in this Declaration.

[18] *Modulation* is ". . . the process of varying a carrier signal, typically a [signal in the shape of a sine wave], in order to use that signal to convey information . . . . There are several reasons to modulate a signal before transmission in a medium. These include the ability of different users sharing a medium (multiple access), and making the signal properties physically compatible with the propagation medium." *See* http://en.wikipedia.org/wiki/Modulation (Exhibit H).

optic cable without detection. All of these characteristics are felt to make fiber more reliable and more secure than copper.

54. At the same time, these characteristics mean that law enforcement has to work harder to implement lawful intercept. The Hollywood image of an FBI agent with a pair of alligator clips is a thing of the past.

55. This is one of the main reasons why CALEA obligates carriers to instrument their networks in order to support requests for lawful intercept. Lawful intercept in today's world depends on the cooperation of the carrier.

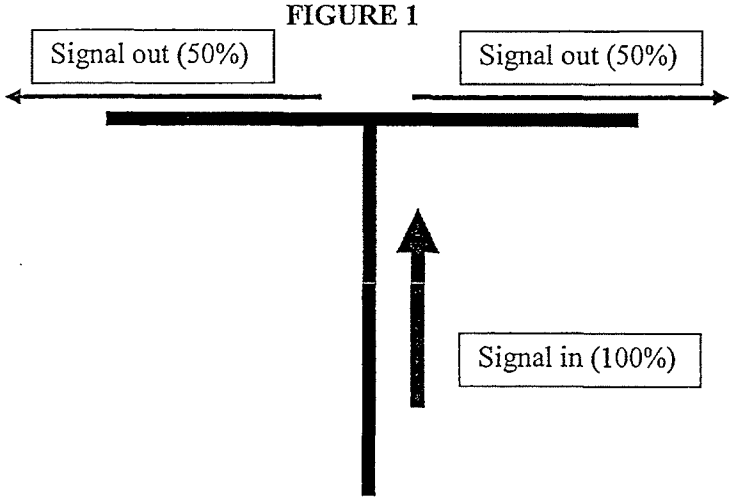
56. In this case, the splitter (described below) provides an equivalent function to that of the alligator clips. However, instead of capturing traffic to a single target, these splitters collectively transferred all or substantially all of AT&T's off net IP-based traffic[19] (so-called Internet *peering*[20] traffic to other Internet backbones) to a secure room.

57. A splitter is a standard bit of optical gear. The simplest form is a "T" – one signal comes in, two signals go out. The splitters in this case were 50/50 splitters, which is to say that they split the signal such that 50% went to each output fiber. *See* the figure immediately below.

[19] The basis for this statement is developed over the balance of this Declaration. Traffic from one AT&T customer to another AT&T customer is *on net* traffic; traffic from an AT&T customer to a customer of some other ISP is in general *off net* traffic. As previously noted, all Internet traffic is *IP-based*, *i.e.* based on the Internet Protocol. I expand on this discussion in the section in which I discuss "Traffic captured."

[20] Again, peering is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers.

FIGURE 1



58. To the layman, it may seem strange that one can split a signal and still use both portions. In everyday life, if we divide something in half, each half is in some sense less than the whole. It is important to remember that, in this case, what is important is the bits (the information carried), not the underlying medium. This is more akin to making a copy of an audio CD – the CD that has been copied is not harmed by being copied. The copy contains the same information as the original.

59. Opto-electronic equipment is routinely designed to recover as much information as possible from weakened signals in order to attempt to compensate for *attenuation*[21] (weakening, or loss of "punch") of the signals over distance.

60. The AT&T designers were well aware that splitting the signal would make it weaker. They expected a loss of 4 dB[22] as a direct result of splitting the signal in two, and a loss of an additional 2 dB due to possible inefficiencies in the process – think of this latter loss as being the equivalent of friction in a mechanical device. This makes for a combined loss of 6 dB. As long

[21] "In telecommunication, *attenuation* is the decrease in intensity of a signal, beam, or wave as a result of absorption of energy and of scattering out of the path to the detector, but not including the reduction due to geometric spreading." *See* http://en.wikipedia.org/wiki/Attenuation (Exhibit I).

[22] dB is the standard abbreviation for decibel. "The decibel (dB) is a measure of the ratio between two quantities, and is used in a wide variety of measurements in acoustics, physics and electronics. . . . It is a "dimensionless unit" like percent. Decibels are useful because they allow even very large or small ratios to be represented with a conveniently small number. This is achieved by using a logarithm." *See* http://en.wikipedia.org/wiki/Decibel (Exhibit J).

as the loss was less than 7 dB, they presumably expected it to be within the normal operating tolerances of the devices on both ends, so they apparently made no provision to correct for the loss. They required technicians to carefully record signal levels before and after the cut (the insertion of the splitters into the operating network), and to report any loss of signal great enough to cause problems to the Network Operations Center (NOC) in Bridgeton, New Jersey.[23]

61. For the work that was described in the Klein Exhibits, each high speed circuit was apparently comprised of multiple fiber optic cables. AT&T chose to connect the cables associated with certain circuits to the splitters, and thereby to divert or copy the signals carried on those circuits. They presumably chose not to connect the cables associated with other circuits to the splitters, and thereby to refrain from diverting or copying the signals associated with those circuits.

62. In the context of the SG3 Configurations, the new splitters and a collection of optical cross-connect cables directed 50% of the signal to complete the same path that the signal had previously taken (from the CBB router to the optical transmission equipment), and directed the other 50% of the signal to the SG3 Equipment.[24] This arrangement enabled the circuits to continue to function just as they previously had, but also made the signals available to the SG3 Equipment.

63. The splitter configuration that AT&T used is routinely available from a major supplier of equipment for electronic communications, ADC. *See* line 1 of page 4 of ADC's brochure "Value-Added Module System: LGX[25] Compatible," available at http://www.adc.com/Library/Literature/891_LGX.pdf (Exhibit K).

SUMMARY OF THE ARCHITECTURE OF THE SG3 CONFIGURATION AND ITS DATA CONNECTIVITY

64. In this section, I provide a summary overview of the architecture of the SG3 Configuration and its data connectivity, based on the Klein Declaration, the Klein Exhibits, and my professional expertise. More details are provided in later sections of this declaration.

---

[23] *See* Klein Exh. A, p. 10.

[24] See, for instance, Figure 5 on page 11 of Klein Exhibit A. Note, too, that the tables on pages 6 and 7 of Klein Exhibit C refers to "50/50 Dual Splitters."

[25] The LGX refers to the format of the physical rack into which the equipment is designed to be deployed. Lucent developed the LGX format. LGX stands for Light Guide Crossconnect.

65. The Klein Declaration refers to a "secret" room being constructed within AT&T Corp.'s Folsom Street Facility, called the "SG3 Secure Room." Klein Decl., ¶ 12.

66. While Mr. Klein worked at the Folsom Street Facility, where he oversaw its WorldNet Internet room,[26] his duties included the installation of new fiber-optic circuits with respect to AT&T's WorldNet Internet service.[27] Klein Decl., ¶¶ 15, 20.

67. In the course of his employment by AT&T, Mr. Klein reviewed the three documents collectively referred to as the Klein Exhibits. Klein Decl., ¶¶ 25-26, 28.

68. The SG3 Configuration, for purposes of my declaration and expert opinions, includes the following basic elements: a room referred to in the Klein Declaration as the "SG3 Secure Room," *id.*, ¶ 12 and Klein Exh. C, p. 46, "SG3 Room," *id.*, p. 45, "SG3 Room LGX," *id.*, p. 13, "SG3 Equipment Room," *id.*, p. 41, and "SG3 Equipment," *see* Klein Decl., Exh. A, p. 10, Fig. 4; sophisticated computers and other electronic devices located in or to be installed in this room; sophisticated routers and switches capable of switching traffic among the computing systems in the room, and also to other locations; and cables associated with data circuits entering and exiting this room.

69. The SG3 Secure Room that Mr. Klein describes in his declaration is fully consistent with the various SG3 rooms referred to in the Klein Exhibits.

70. The Klein Exhibits describe procedures for splitting or diverting peering communications traffic associated with AT&T Corp.'s Common Backbone (CBB) fiber-optic network by means of splitters[28] that fed into the SG3 Secure Room.

71. By following these procedures, all the communications carried on the associated fiber optic circuits were diverted or copied to the SG3 Secure Room and could be made available

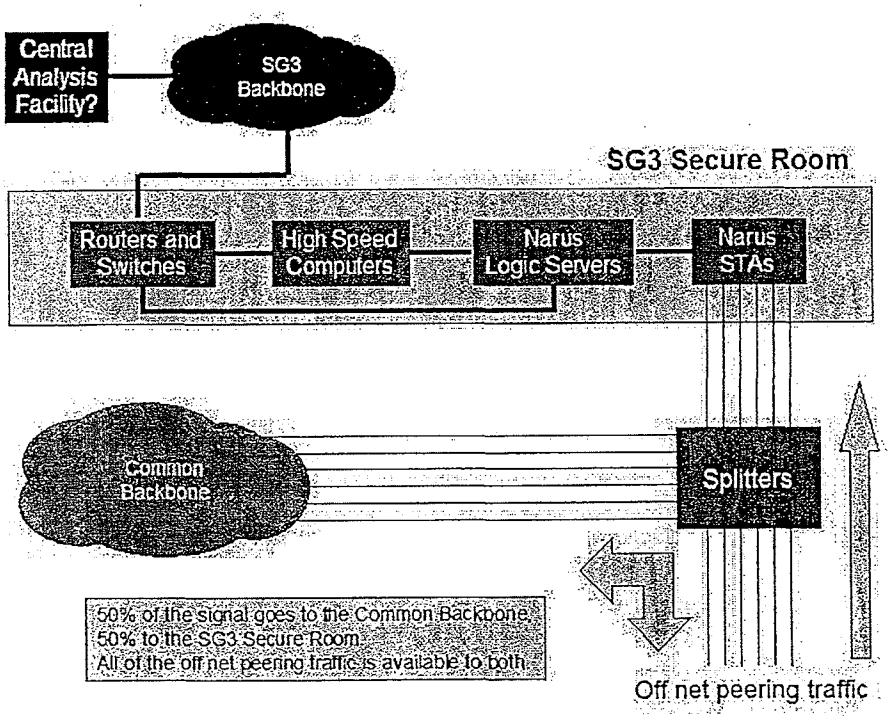
[26] The WorldNet Internet room and its equipment as described by Mr. Klein is a facility for transmitting both domestic and international wire or electronic communications by electromagnetic, photoelectronic or photooptical means. Klein Decl., ¶¶ 15, 19, 22.
[27] The AT&T WorldNet Internet service provides its users with the ability to send or receive email, to browse the web, and to send or receive other wire or electronic communications.
[28] I explained the function of a *splitter* earlier in this declaration, in the section on "Background – Fiber Optics". The T splitters used by AT&T apparently sent 50% of the input signal to each of two optic fiber cables, one of which conveyed the traffic to the SG3 Secure Room.

to any devices in that room.

72. With respect to the SG3 Secure Room in San Francisco, the process resulted in the diversion of all, or substantially all, of AT&T's peering traffic at the Folsom Street San Francisco facility to SG3 equipment, with no significant adverse impact on AT&T's continuously operating CBB Internet backbone.

73. The figure below helps to clarify these relationships. Splitters take the peering traffic from other networks ("off net" traffic) and route 50% of the signal to the CBB, and 50% of the signal to the SG3 Secure Room. Even though only 50% of the *signal* goes to each side of the split, all of the associated *traffic* is available both to the CBB and to the equipment in the SG3 Secure Room.

FIGURE 2



74. The Klein Exhibits also list equipment linked to or contained in the SG3 Secure Room. These include sophisticated computers and other electronic equipment. See Klein Exh. C, p. 3 ("cabinet naming"). At the same time, the Klein Exhibits do not indicate the quantities of

equipment, nor do they indicate the precise interconnections between them; consequently, the connections depicted within the SG3 Secure Room in Figure 2 should be considered to be suggestive but not necessarily exact.

75. An important group of devices in the SG3 Secure Room is the Narus STA 6400, which is a "semantic traffic analyzer," and the Narus Logic Server.[29] As I explain in more detail below, the Narus system is designed to apply logical tests to large volumes of data in real time. It is well suited to the initial screening function of a comprehensive surveillance system – in fact, surveillance is one of the system's primary functions.[30]

76. The Klein Exhibits also refer to the "SG3 backbone" and to the "SG3 backbone circuit[s]."[31] Klein Exh. C, pp. 6, 12, 42. As I explain in more detail below, it is highly likely that this SG3 backbone provides a fiber-optic network connected to the SG3 Secure Room, but separate and distinct from the CBB. In other words, while the SG3 Secure Room is connected to the CBB (from which it receives communications), it is also connected to another network, and signals can be sent out of or into the SG3 Secure Room over the SG3 backbone.

77. In sum, the general architecture of the SG3 Configuration is that communications on the CBB are split by means of splitters in a splitter cabinet, and that these communications feed into the SG3 Secure Room where they can be processed by the equipment in the SG3 Secure Room. At the same time, the SG3 backbone provides a separate, two-way channel of communication with the SG3 Secure Room. The documents reviewed do not, however, indicate what entities can receive signals or information from or send signals or information into the SG3 Secure Room via the SG3 backbone. I consider it highly probable that one or more Centralized Processing Facilities exist, as shown in Figure 2, but that belief is based on the nature of the job that the Narus system is designed to do, rather than being based on the Klein Exhibits themselves.

---

[29] See Klein Exh. C, p. 3 ("cabinet naming"). The Narus Logic Server is apparently implemented in conjunction with a Sun V880 computing system, possibly as software running on the Sun V880.

[30] See http://www.narus.com/solutions/IPanalysis.html (Exhibit L).

[31] In the text, both the SG3 backbone circuits and the peering circuits are referred to in the singular. I believe that these are grammar errors on the part of the author, and that both should have appeared in the plural.

CAPABILITIES OF THE SAN FRANCISCO SG3 CONFIGURATION

78. In this section, I explain my expert opinions about the activities likely to be occurring in the SG3 Secure Room in San Francisco.

79. In order to understand the capabilities of this configuration, it is particularly important to understand the capabilities of the Narus *Semantic Traffic Analyzer (STA)* and the Narus Logic Server. Narus's website provides singularly little information about their offerings, but a few public sources provide useful supporting detail, notably including a presentation that Narus made to the European SCAMPI project in May, 2004, and a Narus presentation available on the website of Narus's reseller IBM.[32]

80. These devices are designed to capture data directly from a network, apply a structured series of tests against the data, and respond appropriately. According to the Narus website, "One distinctive capability that Narus is known for is its ability to capture and collect data at true carrier speeds. Every second, every minute and everyday, Narus collects data from the largest networks around the world. To complement this capability, Narus provides analytics and reporting products that have been deployed by its customers worldwide. They involve powerful parsing algorithms, data aggregation and filtering for delivery to various upstream and downstream operating and support systems. They also involve correlation and association of events collected from numerous sources, received in multiple formats, over many protocols, and through different periods of time."[33]

81. Given the very high data rates that are supported, it is likely that many sophisticated techniques are used to accelerate the processing.

82. The Narus presentation on IBM's web site[34] makes it clear that the Narus system has the ability to inspect user application data (i.e. content), and not merely protocol headers. In this context, it is worth noting that references to layer numbers reflect the OSI Reference Model,

---

[32] *See* http://www.ist-scampi.org/events/workshop-2004/poell.pdf (Exhibit M), and http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf (Exhibit N).

[33] See http://www.narus.com/solutions/IPanalysis.html (Exhibit L).

[34] See http://www-03.ibm.com/industries/telecom/doc/content/bin/tc_using_narus_ip_sept_2005.pdf (Exhibit N).

where levels 5 through 7 correspond to the application[35]:

> The Narus solution is multi-tiered. Within the platform are the first two tiers; the third tier is the application that the platform is enabling. The two Narus tiers or layers are:
>
> • Collection
> • Processing
>
> **Collection**
> The collection layer in the Narus solution consists of High Speed Analyzers which connect to the network at the points where the traffic to be monitored can be most efficiently accessed. The Narus HSA's are passive and as such have zero impact on the service delivery. The HSA's analyse each and every IP packet looking at the OSI layer 2 to layer 7 data and extract layer 4 flows and ***layer 7 application data*** [emphasis added] for every IP session. Appropriate layer 4 and layer 7 data is packaged up and passed to the downstream processing layer as Narus vectors.
>
> **Processing**
> The processing layer in a Narus deployment is the LogicServer. The LogicServer process runs RuleSets which are programs that apply the business logic to the Narus vectors passed by the collection layer.

83. The statements in the IBM document make clear that the Narus system is well suited to process huge volumes of data, including user content, in real time. It is thus well suited to the capture and analysis of large volumes of data for purposes of surveillance.

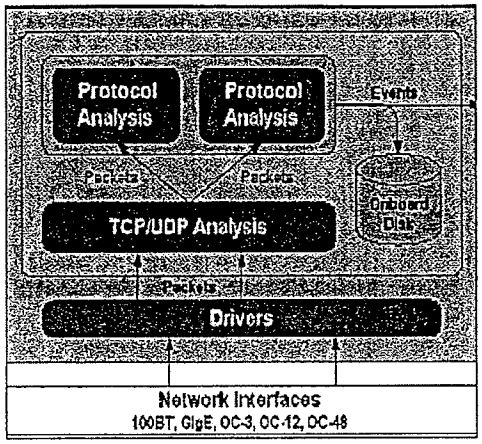
84. The following figure, which is taken from the Narus presentation to SCAMPI, makes it clear that the system, in addition to its other capabilities, is designed to identify traffic of interest and to act on it. It has the ability to store interesting traffic to the onboard disk that is part of the system.

---

35 The Narus website is consistent with this assessment. "Stateful, Real-Time analysis of all of the traffic, Layer 3 to Layer 7 stack". The reference is to the largely obsolete OSI Reference Model of Interconnection, where levels 5 through 7 correspond to the application. See http://www.narus.com/platform/index.html (Exhibit O). For a non-technical explanation of protocol layering in the context of the Internet, *see* section 2 of my paper "Evolving Core Capabilities of the Internet," *Journal on Telecommunications and High Technology Law*, 2004 (Exhibit G).

FIGURE 3

Semantic Traffic Analyzer



85. In addition to its real time capabilities, the Narus offering can subsequently analyze large volumes of data in order to reconstruct session content as needed from the captured collections of packets. This would include e-mail, web browsing, voice over IP (VoIP), and other common kinds of Internet communication.[36]

86. It would, in my judgment, be an error to evaluate the capabilities of this configuration – substantial though they are – solely on the basis of the equipment deployed by AT&T to the SG3 Room. The AT&T documents clearly indicate the presence of an SG3 *backbone* network, apparently operating at OC-3 speeds (155 Mbps).[37] This network, while much smaller than AT&T's CBB Internet backbone network, is nonetheless quite substantial.

87. The SG3 backbone was logically distinct from the AT&T Common Backbone (CBB), but this does not necessarily mean that it had dedicated physical transmission facilities. It most probably operated over AT&T's standard optical fiber-based transmission systems, but using different high speed services – in effect, different circuits – than the CBB. If this network were carrying nothing more than a subset of AT&T's normal commercial traffic, they might not have

---

[36] Narus forensics, for example, "[r]econstructs and renders IP data captured with NarusDA (Directed Analysis), NarusLI (Lawful Intercept) or obtained from other data sources: Visually rebuilds or renders web pages and sessions; Presents e-mail with the header, body and attachments; Plays back streaming video or a VoIP call web session or other interactive medium." *See* http://www.narus.com/solutions/NarusForensics.html (Exhibit P).

[37] Klein Exh. C, pp. 6, 12, 42.

felt the need to do more – it has long been considered permissible to transmit *Sensitive but Unclassified Information (SUCI)* over separate fiber-based transmission paths. Had there been greater sensitivity about the data, it might have been protected in other ways, for instance by means of link encryption.

88. The obvious and natural design for a massive surveillance system for IP-based data, and the one most cost-effective to implement, would in my judgment be comprised of the following elements: (1) massive data capture at the locations where the data can be tapped, (2) high speed screening and reduction[38] of the captured data at the point of capture in order to identify data of interest, (3) shipment of the data of interest to one or two central collection points for more detailed analysis, and (4) intensive analysis and cross correlation of the data of interest by very powerful processing engines at the central location or locations. The AT&T documents demonstrate that equipment that is well suited for the first three of these tasks was deployed to San Francisco and, with high probability, to other locations. I infer that the fourth element also exists at one or more locations.

89. Staff to analyze the data would probably be based at the central locations. There would be no need to station analysts (as distinct from field support personnel) in the SG3 rooms where the data was collected. It is likely that the data were directly available for analysis by staff of the agency that funded the SG3 deployment (which runs counter to normal practice in the case of CALEA); otherwise, there would have been no need for a private SG3 backbone, separate from the CBB.

90. The SG3 technology could potentially be used in a number of different ways, some of which could be welfare-enhancing. The concern that must be raised in this case is that, in conjunction with the diversion of large volumes of traffic described in the Klein Declaration and the Klein Exhibits, this configuration appears to have the capability to enable surveillance and analysis of Internet content on a massive scale, including both overseas and purely domestic traffic.

[38] The Narus STA appears to be ideally suited to this role. It is, as previously noted, designed to apply a large collection of tests against a huge volume of data at very high speed.

TRAFFIC CAPTURED AT SAN FRANCISCO SG3 ROOM

91. In this section, I explain my conclusions about the volume and type of communications traffic gathered by the SG3 Room in San Francisco.

92. The Klein Declaration and Klein Exhibits B & C describe traffic diversions associated with fiber-based circuits in the Folsom Street San Francisco facility.

93. All of the diverted data pertains to AT&T's Common Backbone (CBB), the IP-based network that supports AT&T's Internet access customers, and that also carries AT&T's VoIP services (voice over the Internet).[39] Nothing in the documents suggests that conventional telephony traffic was diverted to the SG3 Configuration.

94. The last page of Klein Exhibit B provides a list of CBB *peering* (defined below) links that were to be split and diverted to the San Francisco SG3 Configuration.

95. Nothing in the documents suggests that AT&T's *on net* traffic – traffic from one AT&T customer to another – was diverted at the time. AT&T may at some point in time have made some provision for its international customers (whose traffic to other AT&T customers would also be on net), but the documents provide no guidance. My assumption is that on net traffic was not diverted during the time frame to which the documents pertain.

96. Before proceeding, it is helpful to introduce and clarify some terms. *Peering* is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers. The Network Reliability and Interoperability Council (NRIC), an advisory panel to the FCC, defined peering in this way:[40]

> *Peering* is an agreement between ISPs to carry traffic for each other and for their respective customers. Peering does not include the obligation to carry traffic to third

---

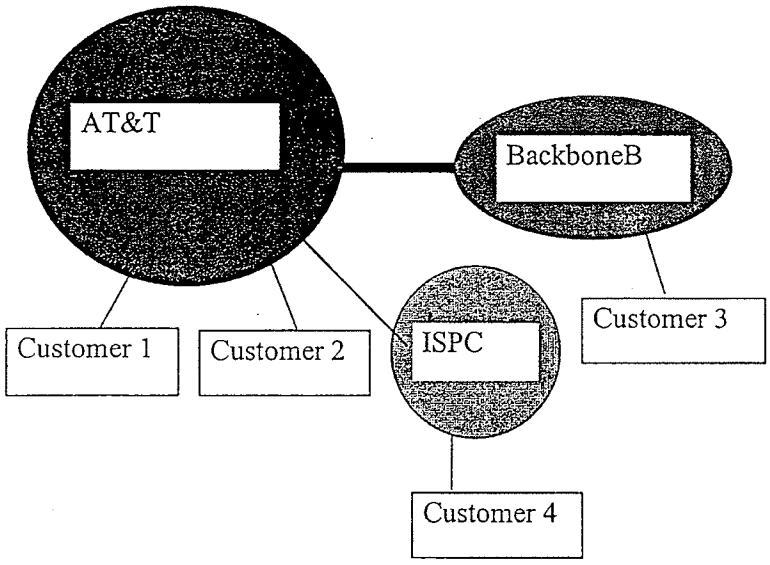
[39] See *In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges,* FCC WC Docket 02-361, Petition of AT&T, at 24 (filed Oct. 18, 2002), at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513386921 (Exhibit Q).

[40] Report of the NRIC V Interoperability Focus Group, an advisory panel to the FCC: "Service Provider Interconnection for Internet Protocol Best Effort Service," page 7, available at http://www.nric.org/fg/fg4/ISP_Interconnection.doc (Exhibit R). *See also* chapter 14 of Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999 (Exhibit S).

> parties. Peering is usually a bilateral business and technical arrangement, where two providers agree to accept traffic from one another, and from one another's customers (and thus from their customers' customers) . . . .

97. In the figure below, AT&T and Backbone B are *peers*. They have agreed to exchange traffic for their respective customers. Traffic from AT&T customer 1 to AT&T customer 2 is *on net* traffic – it remains on AT&T's network. Traffic from AT&T customer 1 to customer 3 (a customer of backbone B) is *off net* traffic.

FIGURE 4



98. In the figure, ISP C is a *transit customer* of AT&T. ISP C pays AT&T to carry its traffic, not only to AT&T customers, but to customers of other ISPs as well (such as, for example, Customer 3). In the context of this discussion, AT&T can regard traffic from Customer 4 to Customers 1 and 2 as being on net, in the sense that it does not traverse a peering connection.

99. It is perhaps also worth noting that AT&T and its peers and their many transit customers do not merely connect to the Internet; rather they *are* the Internet. The Internet is not a single, huge and over-arching network, but rather a collection of independent networks that collectively comprise a worldwide communications stratum.

100. Again, the last page of Exhibit B provides a list of CBB peering links that were to be split and diverted to the San Francisco SG3 Configuration. The sizes of these circuits are listed, with some at OC-3 (155 Mbps), some at OC-12 (620 Mbps), and some at OC-48 (2.5 Gbps). These

are all quite substantial circuits – the OC-48's are apparently on a par with the largest circuits that were in widespread use in AT&T's CBB Internet backbone at the time.

101. Traffic to and from several very large Internet providers at that time (UUNET, Sprint, Level 3 and Cable and Wireless) was delivered over OC-48 circuits. Traffic to and from another group of large providers (Verio, XO, Genuity, Qwest, Allegiance, Abovenet, and Global Crossing) was delivered over OC-12 circuits. Traffic to and from smaller, but still quite substantial, providers (ConXion, Telia and PSINet) was delivered over OC-3 circuits.

102. Large Internet backbone providers typically use direct interconnects (private peering) to exchange traffic with their largest "trading partners in bits," the firms with which they exchange the largest volume of traffic. For providers where the volume of traffic exchange at some location is large enough to warrant peering arrangements, but not large enough to justify the cost of a separate circuit for private peering, it is customary instead to interconnect with multiple peers at a so-called "public peering point" in order to exchange traffic with multiple providers there.[41] AT&T was connected to two public peering points in the San Francisco Bay area: MAE-West and the PAIX. The traffic associated with the OC-3 and OC-12 circuits to these two facilities, respectively, was also diverted to the SG3 configuration.

103. At the point where I left Genuity in July 2001 (some eighteen months before these splitters were deployed), I was intimately familiar with our traffic exchange patterns with other providers. Our measurement instrumentation ranked with the very best in the industry at that time. It is possible to draw many inferences about traffic flows among other providers from one's own traffic exchanges.

104. Based on my experience at Genuity, I believe that the traffic that was diverted represented all, or substantially all, of AT&T's peering traffic in the San Francisco Bay Area.

105. I base my reasoning on the knowledge of Genuity's peering traffic patterns, and on my general understanding of peering traffic patterns in the industry. As of July 2001, our three largest peers were WorldCom, AT&T and Sprint, collectively representing 50-60% of our traffic.

---

[41] *See* Marcus, *Designing Wide Area Networks and Internetworks: A Practical Guide*, Addison Wesley, 1999, pages 280-282 (Exhibit S).

Our next largest peering partners changed somewhat over time, but typically included Qwest, Level3, Verio and Cable and Wireless. Public peering points such as MAE-West represented a small and steadily diminishing percentage of our peering traffic. AT&T had a larger customer base than Genuity, but one might expect the relative proportions to be generally similar, with the obvious exception of AT&T's traffic to itself. The relative sizes of peering circuits on the last page of Klein Exhibit B is not inconsistent with this assumption. Genuity had peering arrangements with 50 to 60 networks, but many of them exchanged relatively little traffic with us. All of our significant peering partners at that time appear on the list on the last page of Klein Exhibit B.

106. I therefore infer either that: (1) all of the networks with which AT&T peered in San Francisco had their traffic intercepted, or else (2) any AT&T peering partners whose traffic was not intercepted most likely were small networks that exchanged very little traffic with AT&T.

107. The traffic intercepted at the Folsom Street facility probably represented a substantial fraction of AT&T's total national peering traffic, but the percentage is unimportant for this analysis.

108. In my judgment, significant traffic to and from the plaintiffs (especially those in the San Francisco Bay Area) would have been available for interception by the SG3 Configuration, even if SG3 had only been implemented in San Francisco. As of the end of 2002, AT&T most likely had West Coast peering to other major backbones at three major locations at most: the San Francisco Bay Area, Los Angeles, and Seattle. As noted above, the major peers were present at Folsom Street, probably representing all or substantially all of AT&T's peering traffic in the San Francisco Bay Area. Off net traffic *from* the plaintiffs would have been handed off to peers at the first available opportunity (a process referred to as "shortest exit" or "hot potato" routing), and thus would with high probability have been handed off through the Folsom Street facility. Off net traffic *to* the plaintiffs could have been presented to AT&T using peering connections at any of perhaps eight different cities, so a significant fraction of the total would have passed through Folsom Street, but not all.

109. I conclude that the designers of the SG3 Configuration made no attempt, in terms of the location or position of the fiber split, to exclude data sources comprised primarily of domestic

data. A fiber splitter, in its nature, is not a selective device – all the traffic on the split circuit was diverted or copied. In my experience, backbone ISPs typically provide a single peering circuit for peering traffic at a given location – they do not provide separate circuits for domestic peering traffic as distinct from international peering traffic. Most of the backbone ISPs that appear in Klein Exhibit B had substantial U.S.-based business, and probably carried significantly more domestic traffic than international.

110. Once the data has been diverted, there is nothing in the data that reliably and unambiguously distinguishes whether the source or destination is domestic or foreign. AT&T would know with near certainty the location of the side of the communication that originated or terminated with its own customer (nearly always domestic in this case), but it would be limited in its ability to determine the location of the other side of the communication. This is because *IP addresses, unlike phone numbers, are not associated with a user's physical location.*

111. There are software programs that attempt to infer physical location from an IP address (a process referred to as *geolocation*). Geolocation is an inherently error-prone process, but some vendors claim, rightly or wrongly, an accuracy of 95% or better. The question of correctness must, however, be considered in the context of the accuracy required. When the FCC considered the geolocation problem in terms of its impact on VoIP users seeking access to emergency services, we were concerned with the possibility of identifying the user's location with sufficient accuracy to enable a policeman or ambulance driver to physically find the caller. In this case, however, it is only necessary to determine whether an IP address is inside the United States. Assuming *arguendo* that the data intercepted by the SG3 Configurations was indeed captured for purposes of surveillance, it is possible that purely domestic communications could have been excluded with a reasonably high success rate. It is nonetheless safe to say that, even had there been a serious attempt to exclude purely domestic communications, some purely domestic communications would have slipped through the filter and been analyzed anyway.

112. The documents provide no basis on which to determine whether geolocation was attempted. Given (under the foregoing assumptions) that all of the international data was going to be evaluated by a sophisticated high speed inference engine (the Narus system) in any case, the

simpler, cheaper and more natural engineering approach would be to use the Narus system to evaluate all of the data, both domestic and foreign, and to leave it to the inference engine to determine which data was interesting.

NUMBER OF LOCATIONS

113. The Klein Declaration states that splitter cabinets were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego. Unlike most statements in the Klein Declaration, this one is not based on his first hand knowledge. It is therefore appropriate to consider first, whether the assertion is plausible, and second, how large a total deployment it implies.

114. Based on my assessment of the AT&T documents, I consider the assertion to be plausible, and to be consistent with an overall national AT&T deployment to from 15 to 20 sites, possibly more.

115. Klein Exhibit B talks about general AT&T naming conventions, and says: "Since this document is designed to cover all sites, this uniform naming convention will be used. Site-specific engineering will use the LGX FIC[42] code rather than the naming."[43] This emphasis on a standardized, cookie-cutter approach is consistent with AT&T standard practice, but also implies a planned deployment to multiple sites, surely more than two or three.

116. All of these documents need to be understood in terms of AT&T practices and priorities. AT&T is used to operating networks on a large scale, with centralized highly skilled engineers and with a field force at a lower skill level. This implies the need for a highly structured approach to describing the work to be done, and precise, meticulous instructions. AT&T had clearly gone to great lengths to standardize the design of their CBB locations as much as possible; nonetheless, for a variety of reasons, the locations were not identical. The directions therefore try to strike a balance between first describing the general case for all locations, and then providing site-specific directions that apply the general directions to the circumstances of a particular CBB

[42] As previously note, the LGX refers to an equipment rack. I infer that the FIC code refers to an AT&T convention that assigns a unique and unambiguous identifier that is suitable for site-specific work.

[43] Klein Exh. B, p. 4.

location.

117. Page 5 of Klein Exhibit A discusses the various racks (LGXes) involved, and says of the Network Facing LGX: "In a majority of cases (possibly all) this will be LLGX4." (Note that the racks associated with AT&T's Common Backbone [CBB] are assigned sequential identifiers from LLGX1 to LLGX14.) If the planned deployment were for only two or three sites, the universality of LLGX4 would not have been in doubt. This again hints at a large enough deployment that it was inconvenient to check all of the necessary background plans.

118. On the same page, Klein Exhibit A refers to four different rack arrangements that could be present at any given site. On site staff would only need to familiarize themselves with the single configuration present at their site. This implies an absolute minimum of four sites; however, I consider it unlikely that they would go to this much trouble in crafting such general language if that were the case. Klein Exhibit A specifically states on page 17: "The only site with LGX Arrangement 4 is Atlanta." The absence of similar statements for Arrangements 1, 2 and 3 implies that there are two or more instances of each of those rack arrangements. Again, this is consistent with a deployment to 15 to 20 SG3 Room sites if not more.

TRAFFIC CAPTURED BY MULTIPLE SG3 ROOMS

119. I have already explained that an enormous amount of Internet traffic is likely to have been captured by the devices in the SG3 Room in San Francisco. I now briefly consider the volume of Internet traffic that would be captured if there were multiple SG3 rooms.

120. Assuming that AT&T deployed SG3 Configurations to as many locations as appears to have been the case, it is highly probable that all or substantially all of AT&T's traffic to and from other Internet providers anywhere in the United States was diverted.

121. If Internet backbone A were carrying x% of all Internet traffic, and if its customers were no more likely to interact with other A customers than with any other provider's customers, then one would expect x% of backbone A's traffic would stay on net and that 100% - x% of A's traffic would go off net (to other providers).[44] In practice, a somewhat higher fraction usually stays

[44] This is the same methodology used in my paper with Laffont, Tirole and Rey. Exhibit D, pp. 373-74.

on net for a variety of reasons.

122. Based on my knowledge of Genuity's traffic flows in 2001, and based also on AT&T's claims that it had grown to become the largest Internet backbone as of late 2002,[45] I would estimate that AT&T was carrying something like 20% of U.S. Internet backbone traffic in late 2002. This estimate reflects the assumption that Genuity's traffic pattern was fairly typical of that of other providers. If AT&T was carrying 20% of all U.S. Internet traffic, and if AT&T customers were no more likely to communicate with other AT&T customers than with customers of any other ISP, then one would expect that about 100% - 20% = 80% of AT&T customer traffic would be destined off net. Given that some traffic tends to stay on net for other reasons – for example, traffic between multiple sites of the same corporation, all of which use AT&T as a provider – I would estimate that somewhere between 60% and 80% of AT&T's customer traffic was going off net.

123. This implies that nearly all of AT&T's international traffic was diverted, with the apparent exception of traffic from an AT&T customer to an overseas AT&T customer.[46]

124. *It also implies that a substantial fraction, probably well over half, of AT&T's purely domestic traffic was diverted, representing all or substantially all of the AT&T traffic handed off to other providers.* This proportion is somewhat less than the 60%–80% estimated above, because it excludes the international traffic.

125. The volume of *purely domestic* communications available for inspection by the SG3 Configurations thus appears to be very substantial. *I estimate that a fully deployed set of SG3 Configurations would have captured something in the neighborhood of 10% of all purely domestic Internet communications in the United States.* This estimate follows from my previous estimates. The SG3 Configurations intercepted more than 50% of all AT&T domestic traffic, which

---

[45] See remarks of Hossein Eslambolchi, AT&T labs president and chief technology officer, quoted in BroadbandWeek Direct at http://www.broadbandweek.com/newsdirect/0208/direct020802.htm, August 2, 2002 ("AT&T has been steadily growing its backbone traffic and now expects to surpass WorldCom as the sector leader in a few months …") (Exhibit T).

[46] To the extent that AT&T has overseas customers, their traffic to other AT&T customers would not appear as peering traffic and therefore would not be intercepted by the SG3 Configurations as described in the AT&T documents.

represented perhaps 20% of all Internet traffic in the United States: 20% * 50% = 10%.

126. It must be emphasized that this estimate does not mean that traffic was intercepted merely for 10% of AT&T customers; rather, it means more than half of all Internet traffic was likely intercepted (at least, at a physical level) for *all* AT&T customers. Moreover, it means that about 10% of all U.S. Internet traffic was physically intercepted for *all* U.S. Internet users, including non-AT&T customers.

127. The estimate of 10% also assumes that only AT&T implemented SG3 Configurations or their equivalent, since the AT&T deployments are the only ones that are demonstrated by the documents that I was asked to review. If other carriers had deployed configurations similar to the SG3 Configurations – feeding in, for example, to the same centralized correlation and analysis center or centers – then the percentage would of course be higher.

ALTERNATIVE REASONS WHY AT&T MIGHT HAVE DEPLOYED THE SG3 CONFIGURATIONS

128. The Klein Declaration states that the SG3 area was a Secure Room, and that only NSA-cleared personnel were permitted to enter. In this section, I consider whether it is credible that the SG3 Room described in the AT&T documents was in fact a secure facility funded by the government. I conclude that it is highly probable.

129. Given the size and the scope of the build-out, and given AT&T's financial difficulties at the time, I consider it highly unlikely that AT&T undertook the development on its own. There is no apparent commercial justification.

130. First, the SG3 Configuration is not useful for carrying Internet traffic. No provider wants to make duplicate copies of the same packets – it costs money to transport the packets, and they provide no corresponding benefits to the user.

131. Second, AT&T might have deployed the SG3 configurations in order to sell security services to their customers. AT&T does in fact offer a service called Internet Protect to its Internet access customers, and the service appears to be based on the Narus offering. Indeed, this is the

rationale indicated on the Narus website.[47] Indications are that the service has not been nearly profitable enough to justify the SG3 expenditure;[48] still it is possible that AT&T might have overestimated demand.

132. This explanation also falls short. The SG3 Configurations were deployed beginning in early 2003, meaning that planning was probably under way six to twelve months earlier, given AT&T process. Internet Protect was not announced until March, 2004.[49] Aside from that, AT&T officials themselves characterized aspects of Internet Protect as something that they had already deployed for other purposes, and only belatedly realized might benefit their customers.[50] All indications are the Internet Protect was an attempt to extract commercial value from a deployment already made – or more likely, from a new deployment using the same technology as the SG3 Configuration – rather than having been the original rationale for the deployment.

133. Third, it is possible that AT&T might have deployed the SG3 configuration in order to meet obligations for lawful intercept. The Narus system can be used for this purpose; however, it is not credible that this was the rationale for the deployment. Far simpler and far less expensive solutions could have met all the limited CALEA requirements that were in force at the time of

---

[47] "AT&T uses NarusSecure to monitor traffic in their backbone, analyzing over 2.6 petabytes of data a day. AT&T is able to provide early warnings to their security center operators, who are able to alert and inoculate their enterprise customers." See http://www.narus.com/solutions/IPsecurity.html (Exhibit U).

[48] "AT&T has packaged that help in a service it calls AT&T Internet Protect, but so far few large agencies have signed up. Buying managed security services from AT&T and other carriers might take some time to catch on, if it ever does, said Timothy McKnight, chief information security officer at Northrop Grumman. "There's a lot of value there, and I agree they should bring it to the table," he said." *See* http://www.fcw.com/article90916-09-26-05-Print (Exhibit V).

[49] http://www.att.com/news/2004/03/22-12972 (Exhibit W).

[50] "Project Gemini, for which development began nearly a year ago, sprang from AT&T's belief that it could better manage customers' security by having the defenses on the company's IP backbone network rather than simply administering security devices on the customers' premises. . . . In addition to the network-based services, AT&T is also working on a security event management system called Aurora that it plans to sell as a software solution. The system relies on the company's Daytona database and is designed to do more than simple event correlation and normalization. . . . AT&T has been using Aurora internally for approximately 18 months, Amoroso said, and only started selling the event management system on a limited basis recently after a customer saw the system and asked for it." Eweek, "Security on the Wire", November 22, 2004, at http://www.eweek.com/print_article2/0,1217,a=139716,00.asp (Exhibit X).

deployment.[51] Workstation solutions, like those in use at Genuity at the time, would have been sufficient to meet legal requirements. The FBI's Carnivore provides a good example of a far more cost-effective solution.[52] (The SG3 Configurations provide a much more capable solution, but in my judgment the company would never have made the substantial incremental investment unless other factors were in play.)

134. Fourth, AT&T might have deployed the system in order to enhance its internal security. This is a somewhat more plausible explanation, but I believe on examination it is far from adequate to explain the investment. It is true that this configuration can be used to protect against distributed denial of service (DDoS) attacks and a number of additional security challenges, but the aggregate benefits do not approach the level of investment made.

135. I considered several alternative hypotheses, including (1) enhanced security for U.S. government customers of AT&T WorldNet; (2) data mining of AT&T customers; and (3) support for sophisticated, possibly application-specific billing and accounting measurements. None of these possibilities would appear to account for the investment that AT&T apparently made in the SG3 Configurations.

136. In sum, I can think of no business rationale in terms of AT&T's own business needs that would likely have justified an investment of this magnitude, nor any combination of rationales.

137. With that in mind, I consider it highly probable that this deployment was externally funded, and I consider the U.S. Government to be the most obvious funding source.

138. The presence of the SG3 backbone is consistent with this assessment. It is far easier to reconcile the presence of a private network with a covert project than it is to explain its presence in the context of normal AT&T operations. AT&T would most likely have used the Common Backbone for routine internal management or operational needs.

139. The SG3 Configuration is, at a technical level, an excellent fit with the requirements

---

[51] The FCC did not impose CALEA requirements on broadband or on Voice over IP (VoIP) until 2005.

[52] Marcus Thomas of the FBI described Carnivore to the North American Network Operators' Group (NANOG) in 2000. The video presentation is available at http://www.nanog.org/mtg-0010/carnivore.html; see also http://videolab.uoregon.edu/nanog/carnivore/.

of a massive, distributed surveillance project. In my opinion, and based on my experience, no other intended purpose explains as well the constellation of design choices that were made.

AT&T'S FINANCIAL CONDITION IN 2003

140. I consider it unlikely that AT&T would have made discretionary investments of this magnitude on its own initiative (with no apparent prospect of return) under any circumstances, but I consider it particularly implausible given the condition of the company in 2003.

141. Lehman Brothers issued investment guidance on AT&T on January 24, 2003, the same day on which Klein Exhibit B was issued. This guidance provides useful historic perspective on the financial state of AT&T as viewed by a knowledgeable and informed observer at the time.[53]

142. In the January 2003 assessment, Lehman Brothers lowered their target stock price from $25 to $20, and recommended that investors underweight AT&T in their portfolios. This reflects a dramatic, precipitous decline. In May 2000, their target had been $400. In January 2001, it was $200. As recently as October 2002, it had been $70.

143. The Lehman Brothers analysis shows a rapid 20% decline in revenues on the part of AT&T Consumer Services, and they predicted a 25-30% decline for 2003. 100% RBOC entry into long distance was already anticipated, as was the FCC's imminent elimination of UNE-P.[54] Lehman Brothers therefore anticipated that AT&T would be forced to exit the Consumer Services business within the year.

144. The profitability of AT&T Business Services was also under pressure – 40% of its revenues came from wholesale long distance voice, where margins were already thin and continuing to decline.

145. In short, most of the financial pressures that ultimately drove AT&T to be acquired by SBC were already evident at the time that these investments were made.

---

[53] A copy of the Lehman Brothers analysis is attached as Exhibit Y to my declaration.

[54] Regional Bell Operating Company (RBOC) entry into long distance would represent increased competition for AT&T's consumer long distance business; the FCC's phasing out of the obligation on RBOCs to provide the Unbundled Network Element Platform (UNE-P) would eliminate AT&T's ability to profitability compete with the RBOCs in offering local services. The combined effect would be to eliminate AT&T's ability to compete with the RBOCs for consumer customers seeking flat rate plans comprising both local service and long distance.

146. Given that there is no apparent revenue justification for the deployment of the SG3 Configurations, I would have expected AT&T to defer discretionary investments at that time. I therefore infer that the deployment was with high probability either externally funded or externally subsidized.

147. This assessment supports the plausibility of the Klein Declaration as regards a government role in the SG3 Configurations.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

///

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed March 29, 2006 at Bonn, Germany.

J Scott Marcus

J. SCOTT MARCUS

CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
KURT OPSAHL (191303)
JAMES S. TYRE (083117)
MARK RUMOLD (279060)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

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

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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

CASE NO. 08-CV-4373-JSW

DECLARATION OF MARK KLEIN WITH REDACTED EXHIBITS FILED IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT

(ORIGINALLY FILED IN THE RELATED CASE OF HEPTING v. AT&T, NO. 06-CV-0676)

Date: November 2, 2012
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

I, Richard R. Wiebe, do hereby declare:

1. I am a member in good standing of the Bar of the State of California and the bar of this Court. I am counsel to plaintiffs in this action and plaintiffs in the related action of *Hepting, et al. v. AT&T Corp., et al.*, N.D. Cal. No. 06-CV-0672. I have personal knowledge of the facts set forth below, except as may be otherwise noted, and if called as a witness I could and would testify competently to them.

2. Attached hereto is the Declaration of Mark Klein and accompanying redacted exhibits, originally filed in the related *Hepting* action. Although portions of the Klein Declaration and its exhibits originally were filed under seal (*Hepting* Dkt. #147; #231), the entire Klein Declaration was unsealed pursuant to stipulation and court order and filed in the public docket (*Hepting* Dkt. #358 & Ex. 1; #361). A redacted version of the exhibits to the Klein Declaration was also unsealed pursuant to stipulation and court order and filed in the public docket (*Hepting* Dkt. #358 & Ex. 2; #361).

3. The Klein Declaration and redacted exhibits attached hereto are the same as those filed in the public docket in the *Hepting* action. The following portions of the Klein Exhibits remaining under seal by order of this Court in the *Hepting* action and are not included in the attached:

a. Exhibit A, pp. 2-3, 5-43.

b. Exhibit B, pp. 1-5, 7-19.

c. Exhibit C, pp. 2, 4-44, 47-58.

(*Hepting* Dkt. # 358 & Exs. 1, 2; #361).

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

Executed at San Francisco, CA on June 29, 2012.

s/ Richard R. Wiebe

Richard R. Wiebe

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
tien@eff.org
KURT OPSAHL (191303)
kurt@eff.org
KEVIN S. BANKSTON (217026)
bankston@eff.org
CORYNNE MCSHERRY (221504)
corynne@eff.org
JAMES S. TYRE (083117)
jstyre@eff.org
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

TRABER & VOORHEES
BERT VOORHEES (137623)
bv@tvlegal.com
THERESA M. TRABER (116305)
tmt@tvlegal.com
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103
Telephone: 626/585-9611
626/ 577-7079 (fax)
Attorneys for Plaintiffs

[Additional counsel appear following the signature page.]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL and ERIK KNUTZEN on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, vs. AT&T CORP., AT&T INC. and DOES 1-20, inclusive, Defendants.	No. C-06-0672-VRW CLASS ACTION DECLARATION OF MARK KLEIN IN SUPPORT OF PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION Date: June 8, 2006 Time: 2:00 p.m. Court: Courtroom 6, 17th Floor Judge: The Hon. Vaughn R. Walker, Chief United States District Judge

FILED UNDER SEAL PURSUANT TO CIVIL LOCAL RULE 79-S

I, Mark Klein, declare under penalty of perjury that the following is true and correct:

1. I am submitting this Declaration in support of Plaintiffs' Motion for a Preliminary Injunction. I have personal knowledge of the facts stated herein, unless stated on information and belief, and if called upon to testify to those facts I could and would competently do so.

2. For over 22 years I worked as a technician for AT&T Corporation ("AT&T"), first in New York and then in California. I started working for AT&T in November 1981 as a Communications Technician.

3. From January 1998 to October 2003, I worked as a Computer Network Associate III at an AT&T facility on Geary Street in San Francisco, CA.

4. From October 2003 to May 2004 I worked as a Communications Technician at an AT&T facility at 611 Folsom St., San Francisco, CA (the "Folsom Street Facility").

5. Previously, I worked as an AT&T Communications Technician from November 1981 to January 1998. I was assigned to AT&T facilities in New York, New York (November 1981 to December 1990), White Plains, NY (December 1990 to March 1991), Pleasanton, CA (March 1991 to May 1993 and March 1994 to January 1998) and Point Reyes, CA (June 1993 to March 1994).

6. I retired from AT&T in May 2004.

7. AT&T Corp. (now a subsidiary of AT&T Inc.) maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day. These facilities allow for the transmission of interstate or foreign electronic voice and data communications by the aid of wire, fiber optic cable, or other like connection between the point of origin and the point of reception.

8. Between 1998 and 2003 I worked in an AT&T office located on Geary Street in San Francisco as one of six Computer Network Associates in the office. The site manager was a management-level technician with the title of Field Support Specialist (hereinafter referred to as FSS #1). Two other FSS people (FSS #2 and FSS #3) also operated from this

office.

9. During my service at the Geary Street facility, the office provided WorldNet Internet service, international and domestic Voice Over IP (voice communications transmitted over the Internet), and data transport service to the Asia/Pacific region.

10. While I worked in the Geary Street facility in 2002, FSS #1 told me to expect a visit from a National Security Agency ("NSA") agent. I and other technicians also received an email from higher management advising us of the pending visit, and the email explicitly mentioned the NSA. FSS #1 told me the NSA agent was to interview FSS #2 for a special job. The NSA agent came and met with FSS #2. FSS #1 later confirmed to me that FSS #2 was working on the special job, and that it was at the Folsom Street Facility.

11. In January 2003, I, along with others, toured the Folsom Street Facility. The Folsom Street Facility consists of three floors of a building that was then operated by SBC Communications, Inc. (now known as AT&T Inc.).

12. While on the January 2003 tour, I saw a new room being built adjacent to the 4ESS switch room. The new room was near completion. I saw a workman apparently working on the door lock for the room. I later learned that this new room being built was referred to in AT&T documents as the "SG3 Secure Room" (hereinafter the "SG3 Secure Room"). The SG3 Secure Room was room number 641A, and measures approximately 24 by 48 feet.

13. The 4ESS switch room is a room that contains a 4ESS switch, a type of electronic switching system that is used to direct long-distance telephone communications. AT&T uses the 4ESS switch in this room to route the public's telephone calls that transit through the Folsom Street Facility.

14. FSS #2, the management-level technician whom the NSA cleared and approved for the special job referenced above, was the person working to install equipment in the SG3 Secure Room.

15. In October 2003, the company transferred me to the AT&T Folsom Street Facility to oversee the WorldNet Internet room, as a Communications Technician.

16. In the Fall of 2003, FSS #1 told me that another NSA agent would again visit our office at Geary Street to talk to FSS #1 in order to get the latter's evaluation of FSS #3's suitability to perform the special job that FSS #2 had been doing. The NSA agent did come and speak to FSS #1. By January 2004, FSS #3 had taken over the special job as FSS #2 was forced to leave the company in a downsizing.

17. The regular AT&T technician workforce was not allowed in the SG3 Secure Room. To my knowledge, only employees cleared by the NSA were permitted to enter the SG3 Secure Room. To gain entry to the SG3 Secure Room required both a physical key for the cylinder lock and a combination code number to be entered into an electronic keypad on the door. To my knowledge, only FSS #2, and later FSS #3, had both the key and the combination code. Regular technicians, including myself, had keys to every other door in the facility because we were often there working alone. We were not given either a key or the combination code for the SG3 Secure Room. On one occasion, when FSS #3 was retrieving a circuit card for me from the SG3 Secure Room, he invited me into the room with him for a couple of minutes while he retrieved the circuit card from a storage cabinet and showed me some poorly installed cable.

18. The extremely limited access to the SG3 Secure Room was highlighted by one incident in 2003. FSS #1 told me that the large industrial air conditioner in the SG3 Secure Room was leaking water through the floor and onto SBC's equipment downstairs, but FSS #2 was not immediately available to provide servicing, and the regular technicians had no access, so the semi-emergency continued for some days until FSS #2 arrived.

19. AT&T provides dial-up and DSL Internet services to its customers through its WorldNet service. The WorldNet Internet room included large routers, racks of modems for AT&T customers' WorldNet dial-in services, and other telecommunications equipment. The equipment in the WorldNet Internet room was used to direct emails, web browsing requests and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service.

20. In the course of my employment, I was responsible for troubleshooting

problems on the fiber optic circuits and installing new fiber optic circuits.

21. The fiber optic cables used by AT&T typically consist of up to 96 optical fibers, which are flexible thin glass fibers capable of transmitting communications through light signals.

22. Within the WorldNet Internet room, high speed fiber optic circuits connect to routers for AT&T's WorldNet Internet service and are part of the AT&T WorldNet's "Common Backbone" (CBB). The CBB comprises a number of major hub facilities, such as the Folsom Street Facility, connected by a mesh of high-speed (OC3, OC12, OC48 and some even higher speed) optical circuits.

23. Unlike traditional copper wire circuits, which emit electromagnetic fields that can be tapped into without disturbing the circuits, fiber optic circuits do not "leak" their light signals. In order to monitor such communications, one has to physically cut into the fiber and divert a portion of the light signal to access the information.

24. A fiber optic circuit can be split using splitting equipment to divide the light signal and to divert a portion of the signal into each of two fiber optic cables. While both signals will have a reduced signal strength, after the split both signals still contain the same information, effectively duplicating the communications that pass through the splitter.

25. In the course of my employment, I reviewed two "Cut-In and Test Procedure" documents dated January 13, 2003 and January 24, 2003, which instructed technicians on how to connect the already in-service circuits to a "splitter cabinet," which diverted light signals from the WorldNet Internet service's fiber optical circuits to the SG3 Secure Room.

26. A true and correct copy of the "Cut-In and Test Procedure" documents are attached hereto as Exhibits A and B. Exhibit A is the January 13, 2003 document, and Exhibit B is the January 24, 2003 document.

27. The light signals from the WorldNet Internet service's optical circuits were split, with a portion of the light signal going through fiber optic cables into the SG3 Secure Room. The AT&T location code of the "splitter cabinet" is 070177.04, which denotes the 7th floor, aisle 177 and bay 04.

28. In the course of my employment, I reviewed a document entitled "Study Group 3, LGX/Splitter Wiring, San Francisco" dated December 10, 2002, authored by AT&T Labs' consultant Mathew F. Casamassima. A true and correct copy of this document is attached hereto as Exhibit C. This document described the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor, and provided diagrams on how the light signal was being split.

29. The circuits that were listed in the "Cut-in and Test Procedure" document dated January 24, 2003 are "Peering Links" that connect the WorldNet Internet network to national and international Internet networks of non-AT&T telecommunications companies.

30. The "Cut-In and Test Procedure" documents provided procedures to "cut-in" AT&T's Peering Links to the splitter and hence to the SG3 Secure Room.

31. Starting in February 2003, the "splitter cabinet" split (and diverted to the SG3 Secure Room) the light signals that contained the communications in transit to and from AT&T's Peering Links with the following Internet networks and Internet exchange points: ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and MAE-West.

32. MAE-West is an Internet nodal point and one of the largest "Internet exchange points" in the United States. PAIX, the Palo Alto Internet Exchange, is another significant Internet exchange point.

33. Internet exchange points are facilities at which large numbers of major Internet service providers interconnect their equipment in order to facilitate the exchange of communications among their respective networks.

34. Through the "splitter cabinet," the content of all of the electronic voice and data communications going across the Peering Links mentioned in paragraphs 29 to 31 was transferred from the WorldNet Internet room's fiber optical circuits into the SG3 Secure Room.

35. The document "Study Group 3, LGX/Splitter Wiring, San Francisco" dated December 10, 2002, listed the equipment installed in the SG3 Secure Room, including such

equipment as Sun servers and Juniper (M40e and M160) "backbone" routers. This list also included a Narus STA 6400, which is a "Semantic Traffic Analyzer."

36. In the course of my employment, I was required to connect new circuits to the "splitter cabinet" and get them up and running. While working on a particularly difficult one with another AT&T technician, I learned that other such "splitter cabinets" were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.

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

DATED: March 28, 2006

Mark Klein

Mark Klein

EXHIBIT A

PERSONAL INFORMATION REDACTED FROM THIS PAGE

AT&T

Labs Connectivity & Net Services

SIMS
Splitter Cut-In and Test Procedure

Issue 2, 01/13/03

Author: Mathew F. Casamassima

Pages A-2 and A-3 redacted.

PERSONAL INFORMATION REDACTED FROM THIS PAGE

SIMS - Splitter Test and Cut-In Procedure
Issue 2, 01/13/03
Mathew F. Casamassima,

1. *Procedure Overview*

A WMS Ticket will be issued by the AT&T Bridgeton Network Operation Center (NOC) to charge time for performing the work described in this procedure document. At some point prior to the splitter cut-in being performed your office will be contacted by the Bridgeton Network Operations Center (NOC) to confirm the WMS Ticket has been received. Bridgeton NOC personnel will again contact OSWF the night of the cut to begin coordination. The work described in the procedure will be supported, on-site, by an IP Field Support Specialist (FSS) from the Day Tech organization.

This procedure covers the steps required to insert optical splitters into select live Common Backbone (CBB) OC3, OC12 and OC48 optical circuits. The splitter insertion will be accomplished by removing existing optical cross-connects and installing new cross-connects all within the CBB LGX complex. The optical splitters will be contained in a standalone cabinet located in the proximity of the CBB LGX complex. The splitters will be pre-cabled by an EF&I vendor to the rear of a dedicated LGX bay (LLGX13) within the CBB LGX complex. A partial installation and test of cross-connects can be done prior to the actual splitter cut-in. This portion of the work can be done outside the CBB maintenance window. An IP FSS member of the Day Tech organization will contact OSWF to schedule the pre-cut portion of the work. Section 2 of this document will describe the pre-cut installation of cross-connects and the pre-cut testing of the new circuit path. The actual cut-in of the splitter will be done during the CBB maintenance window and will be closely coordinated with the Bridge NOC and will be supported, on-site, by an IP FSS member of the Day Tech organization. The actual splitter cut-in is described in Section 3 of this document.

The number of cross-connects required and the final path the circuit will take is dependant on the location of the affected LGX bays within the multiple line-ups of the CBB LGX complex. This procedure will describe all possible splitter cut-in circuit paths. The procedure will also describe the procedures for testing each possible circuit path.

1.1. How to Use this Procedure

This procedure document is quite long. **It is not necessary to read this whole document to do the work.** There are 4 possible LGX arrange that may encounter. By reading section 1.2 below, determine which LGX arrangement applies to the circuit you are working. Then, after reading the introductory paragraphs in Sections 2 and 3, go directly to the subsections within Sections 2 and 3 associated with the LGX arrangement you are dealing with.

1.2. LGX Definition and LGX-Arrangement:

LGX Definition: There are multiple LGX bays affected by this procedure. Within the CBB LGX complex LGX bays follow a specific naming convention (LLGX 1, LLGX2, LLGX3, LLGX4, ...). This naming convention is uniform across sites. Since this document is designed to cover all sites, this uniform naming convention will be used here. Site-specific engineering will use the LGX FIC code rather than the naming. Prior to the start of the work described here the local IP FSS will label the LGX bays with the naming as presented in this document. The following are generic definitions for the LGX bays affected by this procedure:

Pages A-5 to A-43 redacted.

EXHIBIT B

Pages B-1 to B-5
redacted.

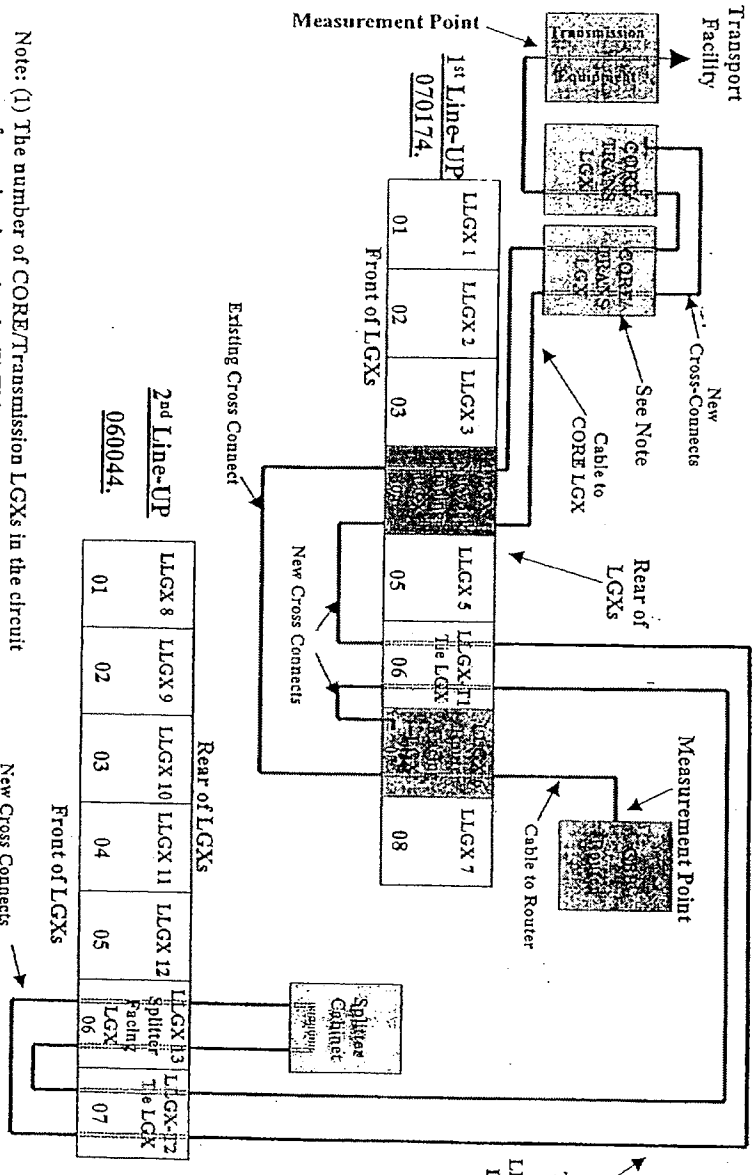


Figure 5 - Arrangement 3 - Circuit Connectivity – Cut Night Measurements
Network Facing & Router Facing LGX in 1st Line-Up / Splitter Facing LGX in 2nd Line-Up
Overhead View of Bays (Applies to Circuits AGEC.671212, AGEC.622360, AGEC.622352, IVEC.517519, IVEC.578278, IVEC.502963, IVEC.547506, IVEC.509396, IVEC.597263, IVEC.502961, IVEC.502960 & IVEC.502947)

Note: (1) The number of CORE/Transmission LGXs in the circuit may vary from circuit to circuit. (2) This arrangement also applies to circuit AGEC.242541 except the Router facing LGX is LLGX 5.

Pages B-7 to B-19 redacted.

Priority	Peering Link	Ckt Type	ID	AS Number	Circuit Comments	Router	Port	Circuit Engineering Change Order Issue Date	Circuit Engineering Complete Date Requested	Circuit Engineering Complete Date Actual	Splitter Pre-Test Date	Splitter In Circuit Date	Splitter Active Date	Comments
1	Conxion	OC-3	AGEC.622352	4544		sffca01ck	POS 1/3	1/22/2003	1/31/2003	1/22/2003	2/4/2003	2/6/2003		
2	Verio	OC-12	IVEC.517519	2914		sffca01ck	POS 3/1	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
3	XO	OC-12	IVEC.578278	2828		sffca01ck	POS 3/2	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
4	Genuity	OC-12	IVEC.502583	1		sffca01ck	POS 3/3	1/23/2003	1/31/2003	1/23/2003	2/4/2003	2/6/2003		
5	Qwest	OC-12	IVEC.647606	209		sffca01ck	POS 5/2	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
6	PAIX	OC-12	IVEC.509396	nap		sffca01ck	POS 8/1	1/30/2003	2/7/2003	1/23/2003	2/11/2003	2/13/2003		
7	Allegiance	OC-12	IVEC.597263	2548		sffca01ck	POS 8/3	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
8	Abovenet	OC-12	IVEC.502361	6461		sffca01ck	POS 9/2	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
9	Global Crossing	OC-12	IVEC.502360	3549		sffca01ck	POS 9/3	1/30/2003	2/7/2003	1/24/2003	2/11/2003	2/13/2003		
10	C&W	OC-48	IWEC.502947	3561		sffca01ck	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
11	UUNET	OC-48	IWEC.509433	701		sffca02ck4	POS 2/0		2/14/2003		2/18/2003	2/20/2003		
12	Level 3	OC-48	IWEC.509434	3356		sffca02ck4	POS 3/0		2/14/2003		2/18/2003	2/20/2003		
13	Sprint	OC-48	IWEC.502438	1239		sffca02ck4	POS 11/0		2/14/2003		2/18/2003	2/20/2003		
14	Telia	OC-3	AGEC.671212	1239		sffca01ck	POS 0/1		2/21/2003		2/25/2003	2/27/2003		
15	PSINet	OC-3	AGEC.622360	174		sffca01ck	POS 0/2		2/21/2003		2/25/2003	2/27/2003		
16	Mae West	OC-3	AGEC.242541	nap		sffca02ck	POS 2/5		2/21/2003		2/25/2003	2/27/2003		

EXHIBIT C

PERSONAL INFORMATION REDACTED FROM THIS PAGE

AT&T

Labs Connectivity & Net Services

Study Group 3
LGX/Splitter Wiring
San Francisco

Issue 1, 12/10/02

Author: Mathew F. Casamassima

Page C-2 redacted.

PERSONAL INFORMATION REDACTED FROM THIS PAGE

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02

Mathew F. Casamassima,

Cabinet Naming:

Equipment	Name
Splitter Cabinet	SPC
LGX Cabinet	LXC
Meta Data Cabinet	MDC
Network Management Cabinet	NMC
Data Filter Cabinet	DFC
Juniper M40E Router Cabinet	JC
Sun V880 Cabinet	S8C
Sun 3800 Cabinet	S3C
Sun Storedge Cabinet	SSC
ADC Chassis For LGX	lxp
ADC Chassis For Splitter	spp
ADC Splitter Module	spl
ADC Bulkhead Module (LGX)	bk
Juniper M160	jp
Juniper M40e	j4
Narus STA 6400	nr
Sun Fire V880/Narus Logic Server	s8
Sun Fire 3800	s3
Sun StorEdge T3	st
Sun StorEdge FC switch	sf
Cisco Catalyst 2924M-XL	cz
BayTech DS9	b9
BayTech RPC22	bv
Brocade SilkWorm 2800 Switch	bz
Lucent LGX	LLGX

Pages C-4 to C-44 redacted.

PERSONAL INFORMATION REDACTED FROM THIS PAGE

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02
Mathew F. Casamassima,

01lxp SG3 LGX Panel to Splitter Cabinet Connectivity

01lxp SG3 LGX Panel Port (In SG3 Room)	Splitter Cabinet Destination	SG3 LGX Designation Card Text	Splitter End Fiber Label Text
1	01spp/Slot 3/port 14	RR 070177.04 01spp/Slot 3/port 14	FROM: 060903.01 01lxp/JK 1 TO: 01spp/Slot 3/port 14
2	01spp/Slot 3/port 13	RR 070177.04 01spp/Slot 3/port 13	FROM: 060903.01 01lxp/JK 2 TO: 01spp/Slot 3/port 13
3	01spp/Slot 3/port 16	RR 070177.04 01spp/Slot 3/port 16	FROM: 060903.01 01lxp/JK 3 TO: 01spp/Slot 3/port 16
4	01spp/Slot 3/port 15	RR 070177.04 01spp/Slot 3/port 15	FROM: 060903.01 01lxp/JK 4 TO: 01spp/Slot 3/port 15
5	01spp/Slot 3/port 18	RR 070177.04 01spp/Slot 3/port 18	FROM: 060903.01 01lxp/JK 5 TO: 01spp/Slot 3/port 18
6	01spp/Slot 3/port 17	RR 070177.04 01spp/Slot 3/port 17	FROM: 060903.01 01lxp/JK 6 TO: 01spp/Slot 3/port 17
7	01spp/Slot 4/port 20	RR 070177.04 01spp/Slot 4/port 20	FROM: 060903.01 01lxp/JK 7 TO: 01spp/Slot 3/port 20
8	01spp/Slot 4/port 19	RR 070177.04 01spp/Slot 4/port 19	FROM: 060903.01 01lxp/JK 8 TO: 01spp/Slot 3/port 19
9	01spp/Slot 4/port 22	RR 070177.04 01spp/Slot 4/port 22	FROM: 060903.01 01lxp/JK 9 TO: 01spp/Slot 3/port 22
10	01spp/Slot 4/port 21	RR 070177.04 01spp/Slot 4/port 21	FROM: 060903.01 01lxp/JK 10 TO: 01spp/Slot 3/port 21
11	01spp/Slot 4/port 24	RR 070177.04 01spp/Slot 4/port 24	FROM: 060903.01 01lxp/JK 11 TO: 01spp/Slot 3/port 24
12	01spp/Slot 4/port 23	RR 070177.04 01spp/Slot 4/port 23	FROM: 060903.01 01lxp/JK 12 TO: 01spp/Slot 3/port 23
13	01spp/Slot 5/port B2	RR 070177.04 01spp/Slot 5/port B2	FROM: 060903.01 01lxp/JK 13 TO:01spp/Slot 5/port B2
14	01spp/Slot 5/port A2	RR 070177.04 01spp/Slot 5/port A2	FROM: 060903.01 01lxp/JK 14 TO:01spp/Slot 5/port A2
15	01spp/Slot 6/port B2	RR 070177:04 01spp/Slot 6/port B2	FROM: 060903.01 01lxp/JK 15 TO:01spp/Slot 6/port B2
16	01spp/Slot 6/port A2	RR 070177.04 01spp/Slot 6/port A2	FROM: 060903.01 01lxp/JK 16 TO:01spp/Slot 6/port A2

AT&T Proprietary

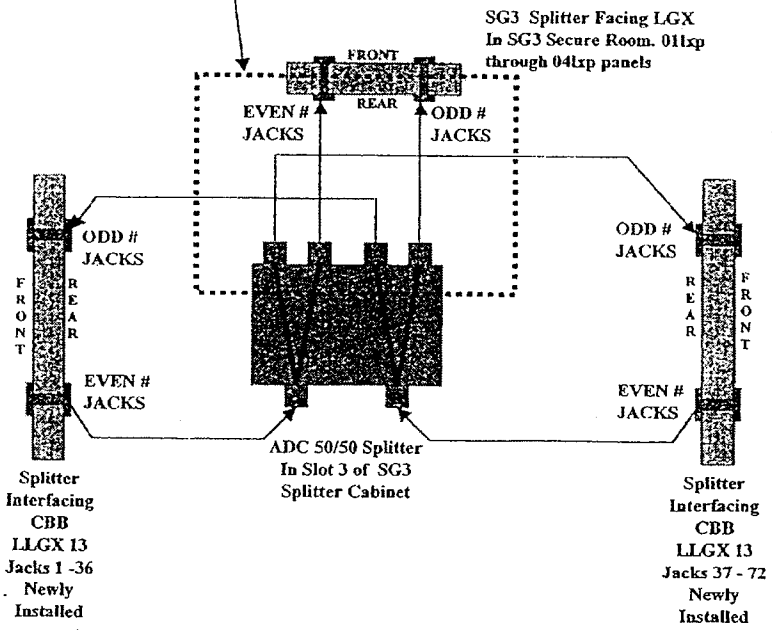
KLEIN C-45

PERSONAL INFORMATION REDACTED FROM THIS PAGE

Study Group 3 LGX/Splitter Wiring, San Francisco
Issue 1, 12/10/02
Mathew F. Casamassima,

Splitter to SG3 LGX Connectivity

The Tables in this section give the splitter to SG3 LGX connectivity as shown with in the bounds of this box.



AT&T Proprietary

KLEIN C-46

Pages C-47 to C-58 redacted.

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
KEVIN S. BANKSTON (SBN 217026)
JAMES S. TYRE (SBN 083117)
454 Shotwell Street
San Francisco, California 94110
Telephone: (415) 436-9333; Facsimile: (415) 436-9993

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

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
425 California Street, Suite 2025
San Francisco, California 94104
Telephone: (415) 433-3200; Facsimile: (415) 433-6382

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all other similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, et al.,

Defendants.

Case No. C-08-4373-VRW

CLASS ACTION

DECLARATION OF CINDY COHN PURSUANT TO FED. R. CIV. P. 56(f) IN OPPOSITION TO GOVERNMENT DEFENDANTS' MOTION TO DISMISS AND FOR SUMMARY JUDGMENT

Date: July 15, 2009
Time: 10:30 a.m.
Dept: 6, 17th Floor
Judge: Vaughn R. Walker

Date Comp. Filed: September 18, 2008

I, CINDY COHN, declare and state:

1. I am an attorney duly licensed to practice law in the courts of the State of California, and I am a member of the bar of this district. I am also Legal Director for the Electronic Frontier Foundation, counsel of record to the Plaintiffs in this action. I am familiar with the records and proceedings in this action as well as the records and proceedings (with the exception of the *in camera, ex parte* materials submitted by the Government) in *In Re National Security Agency Telecommunications Records Litigation*, MDL No. 06-1791 VRW ("the MDL").

2. In *Mohamed v. Jeppesen Dataplan, Inc.*, 563 F.3d 992, (9th Cir. 2009), the Ninth Circuit held that neither the Federal Rules of Civil Procedure nor the state secrets evidentiary privilege established in *United States v. Reynolds*, 345 U.S. 1, 9-10 (1953) would permit a district court to dismiss a well-pleaded complaint at the pleadings stage on the basis of an evidentiary privilege that must be invoked during discovery or at trial. 563 F.3d at 1009. As in *Jeppesen*, the Government here has not filed an answer to the complaint in this case, and discovery has not begun. However, because the Government has styled its motion as a motion to dismiss or alternatively for summary judgment, Plaintiffs are compelled to invoke their rights under Rule 56(f) to have an opportunity to conduct discovery to obtain "facts essential to justify its opposition" to summary judgment.

3. During the course of opposing the Government's motion to dismiss and/or for summary judgment in the MDL, on October 16, 2008, Plaintiffs filed an extensive factual record that establishes the genuine issues as to the material facts surrounding the Government's unlawful surveillance of millions of ordinary Americans. MDL Docket Nos. 479, 486-495. This Court may take judicial notice of the existence of that factual record under Federal Rule of Evidence 201. Plaintiffs summarized that factual record in their Summary of Voluminous Evidence filed under Federal Rule of Evidence 1006, a true and correct copy of which is attached hereto as Exhibit A.[1] Plaintiffs have also filed several Notices of Additional Authorities

[1] The Summary of Voluminous Evidence was filed electronically as MDL Docket No. 481. The evidence itself was filed manually, see MDL Docket No. 484, because it was too voluminous to

containing additional information that has been discovered since the Summary of Voluminous Evidence was filed. MDL Docket Nos. 535, 627 ("Additional Authorities").

4. In addition to the evidence Plaintiffs have already presented, Plaintiffs are entitled under Rule 56(f) to conduct discovery before the Court decides the Government's motion. Plaintiffs respectfully submit that further information supporting their opposition is in the hands of other parties and witnesses, including the Government and its agents and employees and the telecommunications companies and their agents and employees. Discovery is likely to reveal additional facts that will help demonstrate that there are genuine issues of material fact that preclude granting the Government's motion.

5. As the Court ordered in *Al Haramain* (MDL Docket No. 537), if necessary, at least some of Plaintiffs' attorneys would seek a security clearance in order to allow them to conduct discovery.

6. The evidence that Plaintiffs intend to uncover through discovery is available through several channels, as outlined below.

7. Plaintiffs would take the deposition of former government officials who have spoken publicly about the communications carriers' involvement in the NSA's warrantless surveillance, including Defendants Richard B. Cheney, Michael B. Mukasey, John M. McConnell, David S. Addington, Alberto R. Gonzales, John D. Ashcroft and John D. Negroponte, and nonparties Michael Chertoff, Keith B. Alexander, Michael V. Hayden, James Comey, Andrew Card, Jack Goldsmith, John Yoo, Patrick Philbin, Robert S. Mueller III, Thomas M. Tamm, Royce C. Lamberth and Russell Tice. As noted above, if needed Plaintiffs would seek a security clearance to enable them to conduct this discovery in a manner that protects national security.

8. Plaintiffs would seek further written and deposition discovery arising out of the documents summarized in the accompanying Summary of Voluminous Evidence and in the Additional Authorities filed in part to address any claims that any of the information in those documents requires authentication, is hearsay, or is otherwise inadmissible.

---

be filed electronically.

9. For instance, the Summary of Voluminous Evidence references the unclassified nature of 17 paragraphs of notes of then White House Counsel Alberto Gonzales' March 10, 2004 meeting with certain members of Congress known as the "Gang of Eight." The notes discuss legal concerns about the program. As the Inspector General of the Department of Justice reported: "The NSA officials determined that 3 of 21 paragraphs in the notes contains SCI information about the NSA surveillance program [and] 1 paragraph contains SCI information about signals intelligence." Declaration of Kurt Opsahl ("Opsahl Decl.," MDL Docket No. 479) Ex. 7 (Office of the Inspector General, *U.S. Dept. of Justice, Report of Investigation Regarding Allegations of Mishandling of Classified Documents by Att'y Gen. Alberto Gonzales* (Sep. 2, 2008), at p. 10, n.14). Those notes themselves are evidence, or at a minimum are likely to lead to the discovery of admissible evidence, about the scope and legal justification for some portion of the alleged surveillance.

10. Similarly, testimony regarding issues discussed at the March 10, 2004 meeting in Attorney General Ashcroft's hospital room is not classified, since non-cleared personnel were present. *See* Opsahl Decl. Ex. 11 (*Dept. of Justice Oversight*: Hearing before the S. Judiciary Comm. 110th Cong. (Jan 18, 2007)).[2] Again, those issues are either directly relevant to the surveillance alleged in this case or are likely to lead to the discovery of admissible evidence about the facts of the surveillance that led to legal concerns about it at the Department of Justice.

11. Plaintiffs would take depositions of and seek documents from the named sources in the published reports included in the Summary of Voluminous Evidence (Exhibit A hereto) and in the Additional Authorities, regarding those sources' personal knowledge of published or unpublished information or their discussions with or knowledge of other sources of information.

12. To the extent Plaintiffs are able independently to identify any additional sources of evidence, Plaintiffs would seek to obtain declarations from, or propound depositions on written questions to, any unnamed sources, including those quoted in news reports.

13. Plaintiffs would seek discovery regarding the fact of the carriers' interception and

[2] *Available at* http://www.washingtonpost.com/wp-srv/politics/documents/gonzalez_transcript_072407.html.

disclosure of the communications and communications records of the telecommunications companies' customers, including those of the named Plaintiffs and class members.

14. Plaintiffs would take the depositions of Qwest executives including Joseph Nacchio regarding non-privileged discussions with the NSA pertaining to warrantless wiretapping, including content data acquisition. Published accounts note that unlike AT&T, Qwest publicly disclosed that it received a request from the NSA to intercept and disclose customer communications and data, and that it rejected the request.

15. Plaintiffs would take the depositions of Verizon executives regarding non-privileged discussions with the NSA pertaining to warrantless surveillance, including content data acquisition, among other things. For instance, a Verizon Wireless spokeswoman has publicly disclosed that Verizon Wireless received but rejected requests by the NSA that Verizon Wireless intercept and disclose customer communications and data.

16. Plaintiffs would request an inspection of the premises of AT&T's Folsom Street facility under Fed. R. Civ. P. 34, including the WorldNet Internet room, the splitter cable, the inside and outside of the splitter cabinet, and the area outside the SG3 Secure Room. Plaintiffs would also request an inspection of the premises outside of other of AT&T's SG3 rooms, which the record indicates exist in Atlanta, Seattle, San Jose, San Diego, and Los Angeles. Declaration of Mark Klein ¶ 36 (*Hepting v. AT&T,* No. C-06-672 VRW, Docket No. 31 [Vol. 5, Ex. 78, p. 02041]).

17. Plaintiffs would take the depositions (or obtain the sworn declarations) of current or former AT&T employees with knowledge of, and who worked in, the SG3 Secure Room, doing so in a manner that would protect the identities of these witnesses, as needed. Such persons would include, but are not limited to: (1) James W. Russell, who filed a Declaration dated April 10, 2006, under seal due to AT&T trade secret concerns, *see* Notice of Manual Filing, *Hepting* Docket No 42; and (2) the named author of certain exhibits to the Klein Declaration that were also filed under seal. *See* Notice of Manual Filing, *Hepting* Docket No. 31.

18. Plaintiffs would request an inspection of AT&T's facilities housing the Daytona

database and databases used for similar purposes at AT&T and other carriers.

19. Plaintiffs would take depositions of the persons most knowledgeable about AT&T's Daytona database and databases used for similar purposes at AT&T and other carriers.

20. Each of the topics of specific discovery outlined above is highly likely to yield further evidence of genuinely disputed material facts relating to all of Plaintiffs' claims. Specifically, the discovery would lead to evidence regarding the nature and scope of the Government's surveillance program, the timing of efforts to concoct a legal justification for the program, the efforts to mislead Congress and the FISA court about the illegal aspects of the program, and the intention on the part of the individual defendants to violate the Wiretap Act, ECPA, FISA and the Fourth Amendment.

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

Executed at San Francisco, California, this 3rd day of June 2009.

/s/ per General Order 45X.B
CINDY COHN

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
KURT OPSAHL (191303)
KEVIN S. BANKSTON (217026)
JAMES S. TYRE (083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333; Fax: 415/436-9993

RICHARD R. WIEBE (121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: 415/433-3200; Fax: 415/433-6382

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

Attorneys for Plaintiffs

CRB

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, vs. NATIONAL SECURITY AGENCY and KEITH B. ALEXANDER, its Director, in his official and personal capacities; MICHAEL V. HAYDEN, in his personal capacity; the UNITED STATES OF AMERICA; GEORGE W. BUSH, President of the United States, in his official and personal capacities; RICHARD B. CHENEY, in his personal capacity; DAVID S. ADDINGTON, in his personal capacity; DEPARTMENT OF JUSTICE and MICHAEL B. MUKASEY, its Attorney General, in his official and personal capacities; ALBERTO R. GONZALES, in his personal capacity; JOHN D. ASHCROFT, in his personal capacity; JOHN M. MCCONNELL, Director of National Intelligence, in his official and personal capacities; JOHN D. NEGROPONTE, in his personal capacity; and DOES #1-100, inclusive, Defendants.	CASE NO: CLASS ACTION COMPLAINT FOR CONSTITUTIONAL AND STATUTORY VIOLATIONS, SEEKING DAMAGES, DECLARATORY, AND INJUNCTIVE RELIEF DEMAND FOR JURY TRIAL

COMPLAINT

1. Plaintiffs, on behalf of themselves and a class of similarly situated persons, bring this action and allege upon personal knowledge and belief as to their own acts, and upon information and belief (based on the investigation of counsel) as to all other matters, as to which allegations Plaintiffs believe substantial evidentiary support exists or will exist after a reasonable opportunity for further investigation and discovery, as follows:

PRELIMINARY STATEMENT

2. This case challenges an illegal and unconstitutional program of dragnet communications surveillance conducted by the National Security Agency (the "NSA") and other Defendants in concert with major telecommunications companies ("Defendants" is defined collectively as the named defendants and the Doe defendants as set forth in paragraphs 25 through 38 below).

3. This program of dragnet surveillance (the "Program"), first authorized by Executive Order of the President in October of 2001 (the "Program Order") and first revealed to the public in December of 2005, continues to this day.

4. Some aspects of the Program were publicly acknowledged by the President in December 2005 and later described as the "terrorist surveillance program" ("TSP").

5. The President and other executive officials have described the TSP's activities, which were conducted outside the procedures of the Foreign Intelligence Surveillance Act ("FISA") and without authorization by the Foreign Intelligence Surveillance Court ("FISC"), as narrowly targeting for interception the international communications of persons linked to Al Qaeda.

6. The Attorney General and the Director of National Intelligence have since publicly admitted that the TSP was only one particular aspect of the surveillance activities authorized by the Program Order.

7. In addition to eavesdropping on or reading specific communications, Defendants have indiscriminately intercepted the communications content and obtained the communications records of millions of ordinary Americans as part of the Program authorized by the President.

8. The core component of the Program is Defendants' nationwide network of sophisticated communications surveillance devices, attached to the key facilities of telecommunications companies such as AT&T that carry Americans' Internet and telephone communications.

9. Using this shadow network of surveillance devices, Defendants have acquired and continue to acquire the content of a significant portion of the phone calls, emails, instant messages, text messages, web communications and other communications, both international and domestic, of practically every American who uses the phone system or the Internet, including Plaintiffs and class members, in an unprecedented suspicionless general search through the nation's communications networks.

10. In addition to using surveillance devices to acquire the domestic and international communications content of millions of ordinary Americans, Defendants have unlawfully solicited and obtained from telecommunications companies such as AT&T the complete and ongoing disclosure of the private telephone and Internet transactional records of those companies' millions of customers (including communications records pertaining to Plaintiffs and class members), communications records indicating who the customers communicated with, when and for how long, among other sensitive information.

11. This non-content transactional information is analyzed by computers in conjunction with the vast quantity of communications content acquired by Defendants' network of surveillance devices, in order to select which communications are subjected to personal analysis by staff of the NSA and other Defendants, in what has been described as a vast "data-mining" operation.

12. Plaintiffs and class members are ordinary Americans who are current or former subscribers to AT&T's telephone and/or Internet services.

13. Communications of Plaintiffs and class members have been and continue to be illegally acquired by Defendants using surveillance devices attached to AT&T's network, and Defendants have illegally solicited and obtained from AT&T the continuing disclosure of private communications records pertaining to Plaintiffs and class members. Plaintiffs' communications or activities have been and continue to be subject to electronic surveillance.

14. Plaintiffs are suing Defendants to enjoin their unlawful acquisition of the communications and records of Plaintiffs and class members, to require the inventory and destruction of those that have already been seized, and to obtain appropriate statutory, actual, and punitive damages to deter future illegal surveillance.

JURISDICTION AND VENUE

15. This court has subject matter jurisdiction over the federal claims pursuant to 28 U.S.C. § 1331, 18 U.S.C. § 2712, and 5 U.S.C. § 702.

16. Plaintiffs are informed, believe and thereon allege that Defendants have sufficient contacts with this district generally and, in particular, with the events herein alleged, that Defendants are subject to the exercise of jurisdiction of this court over the person of such Defendants and that venue is proper in this judicial district pursuant to 28 U.S.C. § 1391.

17. Plaintiffs are informed, believe and thereon allege that a substantial part of the events giving rise to the claims herein alleged occurred in this district and that Defendants and/or agents of Defendants may be found in this district.

18. **Intradistrict Assignment**: Assignment to the San Francisco/Oakland division is proper pursuant to Local Rule 3-2(c) and (d) because a substantial portion of the events and omissions giving rise to this lawsuit occurred in this district and division.

19. Plaintiffs have fully complied with the presentment of claim provisions of 28 U.S.C. § 2675, as required for their claims under 18 U.S.C. § 2712. Plaintiffs timely served notice of their

claims on the NSA and the Department of Justice on December 19, 2007, and over six months have passed since the filing of that notice.

PARTIES

20. Plaintiff Tash Hepting, a senior systems architect, is an individual residing in Livermore, California. Hepting has been a subscriber and user of AT&T's residential long distance telephone service since at least June 2004.

21. Plaintiff Gregory Hicks is an individual residing in San Jose, California. Hicks, a retired Naval Officer and systems engineer, has been a subscriber and user of AT&T's residential long distance telephone service since February 1995.

22. Plaintiff Carolyn Jewel is an individual residing in Petaluma, California. Jewel, a database administrator and author, has been a subscriber and user of AT&T's WorldNet dial-up Internet service since approximately June 2000.

23. Plaintiff Erik Knutzen is an individual residing in Los Angeles, California. Knutzen, a photographer and land use researcher, was a subscriber and user of AT&T's WorldNet dial-up Internet service from at least October 2003 until May 2005. Knutzen is currently a subscriber and user of AT&T's High Speed Internet DSL service.

24. Plaintiff Joice Walton is an individual residing in San Jose, California. Walton, a high technology purchasing agent, is a current subscriber and user of AT&T's WorldNet dial-up Internet service. She has subscribed to and used this service since around April 2003.

25. Defendant National Security Agency (NSA) is an agency under the direction and control of the Department of Defense that collects, processes and disseminates foreign signals intelligence. It is responsible for carrying out the Program challenged herein.

26. Defendant Lieutenant General Keith B. Alexander is the current Director of the NSA, in office since April 2005. As NSA Director, defendant Alexander has ultimate authority for supervising and implementing all operations and functions of the NSA, including the Program.

27. Defendant Lieutenant General (Ret.) Michael V. Hayden is the former Director of the NSA, in office from March 1999 to April 2005. While Director, Defendant Hayden had ultimate authority for supervising and implementing all operations and functions of the NSA, including the Program.

28. Defendant United States is the United States of America, its departments, agencies, and entities.

29. Defendant George W. Bush is the current President of the United States, in office since January 2001. Mr. Bush authorized and continues to authorize the Program.

30. Defendant Richard B. Cheney is the current Vice President of the United States, in office since January 2001. Defendant Cheney was personally involved in the creation, development and implementation of the Program.

31. Defendant David S. Addington is currently the chief of staff to Defendant Cheney, in office since October 2005. Previously, Defendant Addington served as legal counsel to the Office of the Vice President. Defendant Addington was personally involved in the creation, development and implementation of the Program. On information and belief, Defendant Addington drafted the documents that purportedly authorized the Program.

32. Defendant Department of Justice is a Cabinet-level executive department in the United States government charged with law enforcement, defending the interests of the United States according to the law, and ensuring fair and impartial administration of justice for all Americans.

33. Defendant Michael B. Mukasey is the current Attorney General of the United States, in office since November 2007. As Attorney General, Defendant Mukasey approves and authorizes the Program on behalf of the Department of Justice.

34. Defendant Alberto R. Gonzales is the former Attorney General of the United States, in office from February 2005 to September 2007, and also served as White House Counsel to President George W. Bush from January 2001 to February 2005. Defendant Gonzales was personally involved in the creation, development and implementation of the Program. As Attorney

General, Defendant Gonzales authorized and approved the Program on behalf of the Department of Justice.

35. Defendant John D. Ashcroft is the former Attorney General of the United States, in office from January 2001 to February 2005. As Attorney General, Defendant Ashcroft authorized and approved the Program on behalf of the Department of Justice.

36. Defendant Vice Admiral (Ret.) John M. McConnell is the Director of National Intelligence ("DNI"), in office since February 2007. Defendant McConnell has authority over the activities of the U.S. intelligence community, including the Program.

37. Defendant John D. Negroponte was the first Director of National Intelligence, in office from April 2005 to February 2007. As DNI, Defendant Negroponte had authority over the activities of the U.S. intelligence community, including the Program.

38. At all times relevant hereto, Defendants Doe Nos. 1-100, inclusive (the "Doe defendants"), whose actual names Plaintiffs have been unable to ascertain notwithstanding reasonable efforts to do so, but who are sued herein by the fictitious designation "Doe # 1" through "Doe # 100," were agents or employees of the NSA, the DOJ, the White House, or were other government agencies or entities or the agents or employees of such agencies or entities, who authorized or participated in the Program. Plaintiffs will amend this complaint to allege their true names and capacities when ascertained. Upon information and belief each fictitiously named Defendant is responsible in some manner for the occurrences herein alleged and the injuries to Plaintiffs and class members herein alleged were proximately caused in relation to the conduct of Does 1-100 as well as the named Defendants.

FACTUAL ALLEGATIONS RELATED TO ALL COUNTS

THE PRESIDENT'S AUTHORIZATION OF THE PROGRAM

39. On October 4, 2001, President Bush, in concert with White House Counsel Gonzales, NSA Director Hayden, Attorney General Ashcroft and other Defendants, issued a secret presidential order (the "Program Order") authorizing a range of surveillance activities inside of the United States

without statutory authorization or court approval, including electronic surveillance of Americans' telephone and Internet communications (the "Program").

40. This Program of surveillance inside the United States began at least by October 6, 2001, and continues to this day.

41. The President renewed and, on information and belief, renews his October 4, 2001 order approximately every 45 days.

42. The Program of domestic surveillance authorized by the President and conducted by Defendants required and requires the assistance of major telecommunications companies such as AT&T, whose cooperation in the Program was and on information and belief is obtained based on periodic written requests from Defendants and/or other government agents indicating that the President has authorized the Program's activities, and/or based on oral requests from Defendants and/or other government agents.

43. The periodic written requests issued to colluding telecommunications companies, including AT&T, have stated and on information and belief do state that the Program's activities have been determined to be lawful by the Attorney General, except for one period of less than sixty days.

44. On information and belief, at some point prior to March 9, 2004, the Department of Justice concluded that certain aspects of the Program were in excess of the President's authority and in violation of criminal law.

45. On Tuesday, March 9, 2004, Acting Attorney General James Comey advised the Administration that he saw no legal basis for certain aspects of the Program. The then-current Program authorization was set to expire March 11, 2004.

46. On Thursday, March 11, 2004, the President renewed the Program Order without a certification from the Attorney General that the conduct it authorized was lawful.

47. On information and belief, the March 11 Program Order instead contained a statement that the Program's activities had been determined to be lawful by Counsel to the President Alberto Gonzales, and expressly claimed to override the Department of Justice's conclusion that the Program

was unlawful as well as any act of Congress or judicial decision purporting to constrain the President's power as commander in chief.

48. For a period of less than sixty days, beginning on or around March 11, 2004, written requests to the telecommunications companies asking for cooperation in the Program stated that the Counsel to the President, rather than the Attorney General, had determined the Program's activities to be legal.

49. By their conduct in authorizing, supervising, and implementing the Program, Defendants, including the President, the Vice-President, the Attorneys General and the Directors of NSA since October 2001, the Directors of National Intelligence since 2005 and the Doe defendants, have aided, abetted, counseled, commanded, induced or procured the commission of all Program activities herein alleged, and proximately caused all injuries to Plaintiffs herein alleged.

THE NSA'S DRAGNET INTERCEPTION OF COMMUNICATIONS TRANSMITTED THROUGH AT&T FACILITIES

50. AT&T is a provider of electronic communications services, providing to the public the ability to send or receive wire or electronic communications.

51. AT&T is also a provider of remote computing services, providing to the public computer storage or processing services by means of an electronic communications system.

52. Plaintiffs and class members are, or at pertinent times were, subscribers to and/or customers of AT&T's electronic communications services and/or computer storage or processing services.

53. AT&T maintains domestic telecommunications facilities over which millions of Americans' telephone and Internet communications pass every day.

54. These facilities allow for the transmission of interstate and/or foreign electronic voice and data communications by the aid of wire, fiber optic cable, or other like connection between the point of origin and the point of reception.

55. One of these AT&T facilities is located at on Folsom Street in San Francisco, CA (the "Folsom Street Facility").

56. The Folsom Street Facility contains a "4ESS Switch Room." A 4ESS switch is a type of electronic switching system used to route long-distance telephone communications transiting through the facility.

57. The Folsom Street Facility also contains a "WorldNet Internet Room" containing large routers, racks of modems for AT&T customers' WorldNet dial-up services, and other telecommunications equipment through which wire and electronic communications to and from AT&T's dial-up and DSL Internet service subscribers, including emails, instant messages, Voice-Over-Internet-Protocol ("VOIP") conversations and web browsing requests, are transmitted.

58. The communications transmitted through the WorldNet Internet room are carried as light signals on fiber-optic cables that are connected to routers for AT&T's WorldNet Internet service and are a part of AT&T's Common Backbone Internet network ("CBB"), which comprises a number of major hub facilities such as the Folsom Street Facility that are connected by a mesh of high-speed fiber optic cables and that are used for the transmission of interstate and foreign communications.

59. The WorldNet Internet Room is designed to route and transmit vast amounts of Internet communications that are "peered" by AT&T between AT&T's CBB and the networks of other carriers, such as ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegieance, Abovenet, Global Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and MAE-West. "Peering" is the process whereby Internet providers interchange traffic destined for their respective customers, and for customers of their customers.

60. Around January 2003, the NSA designed and implemented a program in collaboration with AT&T to build a surveillance operation at AT&T's Folsom Street Facility, inside a secret room known as the "SG3 Secure Room".

61. The SG3 Secure Room was built adjacent to the Folsom Street Facility's 4ESS switch room.

62. An AT&T employee cleared and approved by the NSA was charged with setting up and maintaining the equipment in the SG3 Secure Room, and access to the room was likewise controlled by those NSA-approved AT&T employees.

63. The SG3 Secure Room contains sophisticated computer equipment, including a device know as a Narus Semantic Traffic Analyzer (the "Narus STA"), which is designed to analyze large volumes of communications at high speed, and can be programmed to analyze the contents and traffic patterns of communications according to user-defined rules.

64. By early 2003, AT&T—under the instruction and supervision of the NSA—had connected the fiber-optic cables used to transmit electronic and wire communications through the WorldNet Internet Room to a "splitter cabinet" that intercepts a copy of all communications transmitted through the WorldNet Internet Room and diverts copies of those communications to the equipment in the SG3 Secure Room. (Hereafter, the technical means used to receive the diverted communications will be referred to as the "Surveillance Configuration.")

65. The equipment in the SG3 Secure Room is in turn connected to a private high-speed backbone network separate from the CBB (the "SG3 Network").

66. NSA analysts communicate instructions to the SG3 Secure Room's equipment, including the Narus STA, using the SG3 Network, and the SG3 Secure Room's equipment transmits communications based on those rules back to NSA personnel using the SG3 Network.

67. The NSA in cooperation with AT&T has installed and is operating a nationwide network of Surveillance Configurations in AT&T facilities across the country, connected to the SG3 Network.

68. This network of Surveillance Configurations includes surveillance devices installed at AT&T facilities in Atlanta, GA; Bridgeton, MO; Los Angeles, CA; San Diego, CA; San Jose CA; and/or Seattle, WA.

69. Those Surveillance Configurations divert all peered Internet traffic transiting those facilities into SG3 Secure Rooms connected to the secure SG3 Network used by the NSA, and information of interest is transmitted from the equipment in the SG3 Secure Rooms to the NSA based on rules programmed by the NSA.

70. This network of Surveillance Configurations indiscriminately acquires domestic communications as well as international and foreign communications.

71. This network of Surveillance Configurations involves considerably more locations than would be required to capture the majority of international traffic.

72. This network of Surveillance Configurations acquires over half of AT&T's purely domestic Internet traffic, representing almost all of the AT&T traffic to and from other providers, and comprising approximately 10% of all purely domestic Internet communications in the United States, including those of non-AT&T customers.

73. Through this network of Surveillance Configurations and/or by other means, Defendants have acquired and continue to acquire the contents of domestic and international wire and/or electronic communications sent and/or received by Plaintiffs and class members, as well as non-content dialing, routing, addressing and/or signaling information pertaining to those communications.

74. In addition to acquiring all of the Internet communications passing through a number of key AT&T facilities, Defendants and AT&T acquire all or most long-distance domestic and international phone calls to or from AT&T long-distance customers, including both the content of those calls and dialing, routing, addressing and/or signaling information pertaining to those calls, by using a similarly nationwide network of surveillance devices attached to AT&T's long-distance telephone switching facilities, and/or by other means.

75. The contents of communications to which Plaintiffs and class members were a party, and dialing, routing, addressing, and/or signaling information pertaining to those communications, were and are acquired by Defendants in cooperation with AT&T by using the nationwide network of Surveillance Configurations, and/or by other means.

76. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and class members' communications contents and non-content information is done without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

77. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and class members' communications contents and non-content information is done without

probable cause or reasonable suspicion to believe that Plaintiffs or class members have committed or are about to commit any crime or engage in any terrorist activity.

78. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and class members' communications contents and non-content information is done without probable cause or reasonable suspicion to believe that Plaintiffs or class members are foreign powers or agents thereof.

79. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and class members' communications contents and non-content information is done without any reason to believe that the information is relevant to an authorized criminal investigation or to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

80. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and class members' communications contents and non-content information was directly performed, and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

81. On information and belief, Defendants will continue to directly acquire, and/or aid, abet, counsel, command, induce or procure the above-described acquisition in cooperation with AT&T, the communications contents and non-content information of Plaintiffs and class members.

THE NSA'S DRAGNET COLLECTION OF COMMUNICATIONS RECORDS FROM AT&T DATABASES

82. Defendants have since October 2001 continuously solicited and obtained the disclosure of all information in AT&T's major databases of stored telephone and Internet records, including up-to-the-minute updates to the databases that are disclosed in or near real-time.

83. Defendants have solicited and obtained from AT&T records concerning communications to which Plaintiffs and class members were a party, and continue to do so.

84. In particular, Defendants have solicited and obtained the disclosure of information managed by AT&T's "Daytona" database management technology, which includes records concerning both telephone and Internet communications, and continues to do so.

85. Daytona is a database management technology designed to handle very large databases and is used to manage "Hawkeye," AT&T's call detail record ("CDR") database, which contains records of nearly every telephone communication carried over its domestic network since approximately 2001, records that include the originating and terminating telephone numbers and the time and length for each call.

86. The Hawkeye CDR database contains records or other information pertaining to Plaintiffs' and class members' use of AT&T's long distance telephone service and dial-up Internet service.

87. As of September 2005, all of the CDR data managed by Daytona, when uncompressed, totaled more than 312 terabytes.

88. Daytona is also used to manage AT&T's huge network-security database, known as "Aurora," which has been used to store Internet traffic data since approximately 2003. The Aurora database contains huge amounts of data acquired by firewalls, routers, honeypots and other devices on AT&T's global IP (Internet Protocol) network and other networks connected to AT&T's network.

89. The Aurora database managed by Daytona contains records or other information pertaining to Plaintiffs' and class members' use of AT&T's Internet services.

90. Since October 6, 2001 or shortly thereafter, Defendants have continually solicited and obtained from AT&T disclosure of the contents of the Hawkeye and Aurora communications records databases and/or other AT&T communications records, including records or other information pertaining to Plaintiffs' and class members' use of AT&T's telephone and Internet services.

91. The NSA and/or other Defendants maintain the communications records disclosed by AT&T in their own database or databases of such records.

92. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs' and class members' communications records, and its receipt of such disclosure, is done without judicial,

statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

93. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs' and class members' communications records, and its receipt of such disclosure, is done without probable cause or reasonable suspicion to believe that Plaintiffs' or class members have committed or are about to commit any crime or engage in any terrorist activity.

94. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs' and class members' communications records, and its receipt of such disclosure, is done without probable cause or reasonable suspicion to believe that Plaintiffs' or class members are foreign powers or agents thereof.

95. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs' and class members' communications records, and its receipt of such disclosure, is done without any reason to believe that the information is relevant to an authorized criminal investigation or to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

96. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs' and class members' communications records, and its receipt of such disclosure, is directly performed, and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

97. On information and belief, Defendants will continue to directly solicit and obtain AT&T's disclosure of its communications records, including records pertaining to Plaintiffs and class members, and/or will continue to aid, abet, counsel, command, induce or procure that conduct.

CLASS ACTION ALLEGATIONS

98. Pursuant to Federal Rules of Civil Procedure, Rule 23(b)(2), Plaintiffs Hepting, Hicks, Jewel, Knutzen, and Walton bring this action on behalf of themselves and a class of similarly situated persons defined as:

> All individuals in the United States that are current residential subscribers or customers of AT&T's telephone services or Internet services, or that were residential telephone or Internet subscribers or customers at any time after September 2001.

99. The class seeks certification of claims for declaratory, injunctive and other equitable relief pursuant to 18 U.S.C. §2520, 18 U.S.C. §2707 and 5 U.S.C. § 702, in addition to declaratory and injunctive relief for violations of the First and Fourth Amendments. Members of the class expressly and personally retain any and all damages claims they individually may possess arising out of or relating to the acts, events, and transactions that form the basis of this action. The individual damages claims of the class members are outside the scope of this class action.

100. Excluded from the class are the individual Defendants, all who have acted in active concert and participation with the individual Defendants, and the legal representatives, heirs, successors, and assigns of the individual Defendants.

101. Also excluded from the class are any foreign powers, as defined by 50 U.S.C. § 1801(a), or any agents of foreign powers, as defined by 50 U.S.C. § 1801(b)(1)(A), including without limitation anyone who knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore.

102. This action is brought as a class action and may properly be so maintained pursuant to the provisions of the Federal Rules of Civil Procedure, Rule 23. Plaintiffs reserve the right to modify the class definition and the class period based on the results of discovery.

103. **Numerosity of the Class**: Members of the class are so numerous that their individual joinder is impracticable. The precise numbers and addresses of members of the class are unknown to the Plaintiffs. Plaintiffs estimate that the class consists of millions of members. The precise number of persons in the class and their identities and addresses may be ascertained from Defendants' and AT&T's records.

104. **Existence of Common Questions of Fact and Law**: There is a well-defined community of interest in the questions of law and fact involved affecting the members of the class. These common legal and factual questions include:

(a) Whether Defendants have violated the First and Fourth Amendment rights of class members, or are currently doing so;

(b) Whether Defendants have subjected class members to electronic surveillance, or have disclosed or used information obtained by electronic surveillance of the class members, in violation of 50 U.S.C. § 1809, or are currently doing so;

(c) Whether Defendants have intercepted, used or disclosed class members' communications in violation of 18 U.S.C. § 2511, or are currently doing so;

(d) Whether Defendants have solicited and obtained the disclosure of the contents of class members' communications in violation of 18 U.S.C. § 2703(a) or (b), or are currently doing so;

(e) Whether Defendants have solicited or obtained the disclosure of non-content records or other information pertaining to class members in violation of 18 U.S.C. § 2703(c), or are currently doing so;

(f) Whether Defendants have violated the Administrative Procedures Act, 5 U.S.C. §§ 701 *et seq.*, or are currently doing so;

(g) Whether the Defendants have violated the constitutional principle of separation of powers, or are currently doing so;

(h) Whether Plaintiffs and class members are entitled to injunctive, declaratory, and other equitable relief against Defendants;

(i) Whether Plaintiffs and class members are entitled to an award of reasonable attorneys' fees and costs of this suit.

105. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the class because Plaintiffs are or were subscribers to the Internet and telephone services of Defendants. Plaintiffs and all members of the class have similarly suffered harm arising from Defendants' violations of law, as alleged herein.

106. **Adequacy**: Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the members of the class they seek to represent. Plaintiffs have

retained counsel competent and experienced in complex class action litigation and Plaintiffs intends to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the members of the class.

107. This suit may be maintained as a class action pursuant to Federal Rules of Civil Procedure, Rule 23(b)(2) because Plaintiffs and the class seek declaratory and injunctive relief, and all of the above factors of numerosity, common questions of fact and law, typicality and adequacy are present. Moreover, Defendants have acted on grounds generally applicable to Plaintiffs and the class as a whole, thereby making declaratory and/or injunctive relief proper.

COUNT I

Violation of Fourth Amendment—Declaratory, Injunctive, and Equitable Relief

(Named Plaintiffs and Class vs. Defendants United States, National Security Agency, Department of Justice, Bush (in his official and personal capacities), Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

108. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

109. Plaintiffs and class members have a reasonable expectation of privacy in their communications, contents of communications, and/or records pertaining to their communications transmitted, collected, and/or stored by AT&T.

110. Defendants have directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T, without judicial or other

lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

111. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T, without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

112. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs and class members by obtaining judicial or other lawful authorization and by conforming their conduct to the requirements of the Fourth Amendment.

113. By the acts alleged herein, Defendants have violated Plaintiffs' and class members' reasonable expectations of privacy and denied Plaintiffs and class members their right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.

114. By the acts alleged herein, Defendants' conduct has proximately caused harm to Plaintiffs and class members.

115. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' and class members' constitutional rights.

116. On information and belief, the Count I Defendants are now engaging in and will continue to engage in the above-described violations of Plaintiffs' and class members' constitutional rights, and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count I Defendants' continuing unlawful conduct,

and the Count I Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

117. Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count I Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' rights under the Fourth Amendment to the United States Constitution; and award such other and further equitable relief as is proper.

COUNT II

Violation of Fourth Amendment—Damages

(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his personal capacity), Negroponte (in his personal capacity), and one or more of the Doe Defendants)

118. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

119. Plaintiffs have a reasonable expectation of privacy in their communications, contents of communications, and/or records pertaining to their communications transmitted, collected, and/or stored by AT&T.

120. Defendants have directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T without judicial or other lawful

authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

121. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

122. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs by obtaining judicial or other lawful authorization and conforming their conduct to the requirements of the Fourth Amendment.

123. By the acts alleged herein, Defendants have violated Plaintiffs' reasonable expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.

124. By the acts alleged herein, Defendants' conduct has proximately caused harm to Plaintiffs.

125. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' constitutional rights.

126. Plaintiffs seek an award of their actual damages and punitive damages against the Count II Defendants, and such other or further relief as is proper.

COUNT III

Violation of First Amendment—Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants United States, National Security Agency, Department of Justice, Bush (in his official and personal capacities), Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

127. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

128. Plaintiffs and class members use AT&T's services to speak or receive speech anonymously and to associate privately.

129. Defendants directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications without judicial or other lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

130. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

131. By the acts alleged herein, Defendants violated Plaintiffs' and class members' rights to speak and to receive speech anonymously and associate privately under the First Amendment.

132. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs and class members.

133. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' and class members' constitutional rights.

134. On information and belief, the Count III Defendants are now engaging in and will continue to engage in the above-described violations of Plaintiffs' and class members' constitutional rights, and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count III Defendants' continuing unlawful conduct, and the Count III Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

135. Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count III Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' rights under the First Amendment to the United States Constitution; and award such other and further equitable relief as is proper.

COUNT IV

Violation of First Amendment—Damages

(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)

136. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

137. Plaintiffs use AT&T's services to speak or receive speech anonymously and to associate privately.

138. Defendants directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications without judicial or other lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

139. By the acts alleged herein, Defendants violated Plaintiffs' rights to speak and receive speech anonymously and associate privately under the First Amendment.

140. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs.

141. Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' constitutional rights.

142. Plaintiffs seek an award of their actual damages and punitive damages against the Count IV Defendants, and for such other or further relief as is proper.

COUNT V

Violation of Foreign Intelligence Surveillance Act—Declaratory, Injunctive and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

143. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

144. In relevant part, 50 U.S.C. § 1809 provides that:

> (a) Prohibited activities—A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law

except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

145. In relevant part 50 U.S.C. § 1801 provides that:

(f) "Electronic surveillance" means – (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

146. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." (Emphasis added.)

147. 50 U.S.C. § 1812 further provides in relevant part that:

(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which

> electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
>
> (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

148. Defendants intentionally acquired, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of such acquisition, by means of a surveillance device, the contents of one or more wire communications to or from Plaintiffs and class members or other information in which Plaintiffs or class members have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.

149. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition of Plaintiffs' communications.

150. By the acts alleged herein, Defendants acting in excess of their statutory authority and in violation of statutory limitations have intentionally engaged in, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under color of law, not authorized by any statute, to which Plaintiffs and class members were subjected in violation of 50 U.S.C. § 1809.

151. Additionally or in the alternative, by the acts alleged herein, Defendants acting in excess of their statutory authority and in violation of statutory limitations have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or

having reason to know that the information was obtained through electronic surveillance not authorized by statute, including information pertaining to Plaintiffs and class members, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of such acts.

152. Defendants did not notify Plaintiffs or class members of the above-described electronic surveillance, disclosure, and/or use, nor did Plaintiffs or class members consent to such.

153. Plaintiffs and class members have been and are aggrieved by Defendants' electronic surveillance, disclosure, and/or use of their wire communications.

154. On information and belief, the Count V Defendants are now engaging in and will continue to engage in the above-described acts resulting in the electronic surveillance, disclosure, and/or use of Plaintiffs' and class members' wire communications, acting in excess of the Count V Defendants' statutory authority and in violation of statutory limitations, including 50 U.S.C. § 1809 and 18 U.S.C. § 2511(2)(f), and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count V Defendants' continuing unlawful conduct, and the Count V Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

155. Pursuant to *Larson v. United States*, 337 U.S. 682 (1949) and to 5 U.S.C. § 702, Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count V Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' statutory rights, including their rights under 50 U.S.C. §§ 1801 *et seq.*; and award such other and further equitable relief as is proper.

COUNT VI

Violation of 50 U.S.C. § 1809, actionable under 50 U.S.C. § 1810—Damages

(Named Plaintiffs vs. Defendants United States, National Security Agency, Department of Justice, Alexander (in his official and personal capacities), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his official and personal capacities), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his official and personal capacities), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)

156. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

157. In relevant part, 50 U.S.C. § 1809 provides that:

> (a) Prohibited activities—A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

158. In relevant part 50 U.S.C. § 1801 provides that:

> (f) "Electronic surveillance" means – (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio

> communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

159. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." (Emphasis added.)

160. 50 U.S.C. § 1812 further provides in relevant part that:

> (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
>
> (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

161. Defendants intentionally acquired, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of such acquisition, by means of a surveillance device, the contents of one or more wire communications to or from Plaintiffs or other information in which Plaintiffs have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.

162. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition of Plaintiffs' communications.

163. By the acts alleged herein, Defendants have intentionally engaged in, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,

willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under color of law, not authorized by any statute, to which Plaintiffs were subjected in violation of 50 U.S.C. § 1809.

164. Additionally or in the alternative, by the acts alleged herein, Defendants have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute, including information pertaining to Plaintiffs, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of such acts.

165. Defendants did not notify Plaintiffs of the above-described electronic surveillance, disclosure, and/or use, nor did Plaintiffs consent to such.

166. Plaintiffs have been and are aggrieved by Defendants' electronic surveillance, disclosure, and/or use of their wire communications.

167. Pursuant to 50 U.S.C. § 1810, which provides a civil action for any person who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of 50 U.S.C. § 1809, Plaintiffs seek from the Count VI Defendants for each Plaintiff their statutory damages or actual damages; punitive damages as appropriate; and such other and further relief as is proper.

COUNT VII

Violation of 18 U.S.C. § 2511—Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

168. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

169. In relevant part, 18 U.S.C. § 2511 provides that:

> (1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

170. 18 U.S.C. § 2511 further provides that:

> (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

171. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." (Emphasis added.)

172. 50 U.S.C. § 1812 further provides in relevant part that:

> (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
>
> (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

173. By the acts alleged herein, Defendants have intentionally and willfully intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs' and class members' wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

174. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or endeavored to disclose, to another person the contents of Plaintiffs' and class members' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

175. By the acts alleged herein, Defendants have intentionally and willfully used, or endeavored to use, the contents of Plaintiffs' and class members' wire or electronic communications, while knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(d).

176. By the acts alleged herein, Defendants have intentionally and willfully caused, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

177. Defendants have committed these acts of interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications directly or by aiding, abetting, counseling,

commanding, inducing, procuring, encouraging, promoting, instigating, advising, willfully causing, participating in, enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their commission. In doing so, Defendants have acted in excess of their statutory authority and in violation of statutory limitations.

178. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications.

179. Defendants did not notify Plaintiffs or class members of the above-described intentional interception, disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or class members consent to such.

180. Plaintiffs and class members have been and are aggrieved by Defendants' intentional and willful interception, disclosure, divulgence and/or use of their wire or electronic communications.

181. On information and belief, the Count VII Defendants are now engaging in and will continue to engage in the above-described acts resulting in the intentional and willful interception, disclosure, divulgence and/or use of Plaintiffs' and class members' wire or electronic communications, acting in excess of the Count VII Defendants' statutory authority and in violation of statutory limitations, including 18 U.S.C. § 2511, and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count VII Defendants' continuing unlawful conduct, and the Count VII Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

182. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose wire or electronic communications have been intercepted, disclosed, divulged or intentionally used in violation of 18 U.S.C. § 2511, to *Larson v. United States*, 337 U.S. 682 (1949), and to 5 U.S.C. §

702, Plaintiffs and class members seek equitable and declaratory relief against the Count VII Defendants.

183. Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count VII Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' statutory rights, including their rights under 18 U.S.C. § 2511; and award such other and further equitable relief as is proper.

COUNT VIII

Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2520—Damages

(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)

184. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

185. In relevant part, 18 U.S.C. § 2511 provides that:

> (1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

186. 18 U.S.C. § 2511 further provides that:

> (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to

> such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

187. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." (Emphasis added.)

188. 50 U.S.C. § 1812 further provides in relevant part that:

> (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
>
> (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

189. By the acts alleged herein, Defendants have intentionally and willfully intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs' wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

190. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or endeavored to disclose, to another person the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

191. By the acts alleged herein, Defendants have intentionally and willfully used, or endeavored to use, the contents of Plaintiffs' wire or electronic communications, while knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(d).

192. By the acts alleged herein, Defendants have intentionally and willfully caused, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

193. Defendants have committed these acts of interception, disclosure, divulgence and/or use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing, procuring, encouraging, promoting, instigating, advising, willfully causing, participating in, enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their commission.

194. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure, divulgence and/or use of Plaintiffs' communications.

195. Defendants did not notify Plaintiffs of the above-described intentional interception, disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or class members consent to such.

196. Plaintiffs have been and are aggrieved by Defendants' intentional and willful interception, disclosure, divulgence and/or use of their wire or electronic communications.

197. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose wire or electronic communications have been intercepted, disclosed, divulged or intentionally used in violation of 18 U.S.C. § 2511, Plaintiffs seek from the Count VIII Defendants for each Plaintiff their statutory damages or actual damages; punitive damages as appropriate; and such other and further relief as is proper.

COUNT IX

Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2712—Damages Against The United States

(Named Plaintiffs vs. Defendants United States, Department of Justice, and National Security Agency)

198. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

199. In relevant part, 18 U.S.C. § 2511 provides that:

> (1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

200. 18 U.S.C. § 2511 further provides that:

> (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

201. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." (Emphasis added.)

202. 50 U.S.C. § 1812 further provides in relevant part that:

> (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.
>
> (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

203. By the acts alleged herein, Defendants have intentionally and willfully intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs' wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

204. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or endeavored to disclose, to another person the contents of Plaintiffs' wire or electronic communications, knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

205. By the acts alleged herein, Defendants have intentionally and willfully used, or endeavored to use, the contents of Plaintiffs' wire or electronic communications, while knowing or having reason to know that the information was obtained through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(d).

206. By the acts alleged herein, Defendants have intentionally and willfully caused, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

207. Defendants have committed these acts of interception, disclosure, divulgence and/or use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing, procuring, encouraging, promoting, instigating, advising, willfully causing, participating in,

enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their commission.

208. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure, divulgence and/or use of Plaintiffs' communications.

209. Defendants did not notify Plaintiffs of the above-described intentional interception, disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or class members consent to such.

210. Plaintiffs have been and are aggrieved by Defendants' intentional and willful interception, disclosure, divulgence and/or use of their wire or electronic communications.

211. Title 18 U.S.C. § 2712 provides a civil action against the United States and its agencies and departments for any person whose wire or electronic communications have been intercepted, disclosed, divulged or intentionally used in willful violation of 18 U.S.C. § 2511. Plaintiffs have complied fully with the claim presentment procedure of 18 U.S.C. § 2712. Pursuant to 18 U.S.C. § 2712, Plaintiffs seek from the Count IX Defendants for each Plaintiff their statutory damages or actual damages, and such other and further relief as is proper.

COUNT X

Violation of 18 U.S.C. § 2703(a) & (b)—Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

212. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

213. In relevant part, 18 U.S.C. § 2703 provides that:

(a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

214. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in soliciting and obtaining from AT&T, the disclosure to Defendants of the contents of

Plaintiffs' and class members' communications while in electronic storage by an AT&T electronic communication service, and/or while carried or maintained by an AT&T remote computing service, in violation of 18 U.S.C. §§ 2703(a) and/or (b). In doing so, Defendants have acted in excess of their statutory authority and in violation of statutory limitations.

215. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' and class members' communications.

216. Defendants did not notify Plaintiffs or class members of the disclosure of their communications, nor did Plaintiffs or class members consent to such.

217. Plaintiffs and class members have been and are aggrieved by Defendants' above-described soliciting and obtaining of disclosure of the contents of communications.

218. On information and belief, the Count X Defendants are now engaging in and will continue to engage in the above-described soliciting and obtaining of disclosure of the contents of class members' communications while in electronic storage by AT&T's electronic communication service(s), and/or while carried or maintained by AT&T's remote computing service(s), acting in excess of the Count X Defendants' statutory authority and in violation of statutory limitations, including 18 U.S.C. § 2703(a) and (b), and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count X Defendants' continuing unlawful conduct, and the Count X Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

219. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief against the Count X Defendants.

220. Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count X Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' statutory rights, including their rights under 18 U.S.C. § 2703; and award such other and further equitable relief as is proper.

COUNT XI

Violation of 18 U.S.C. § 2703(a) & (b), actionable under 18 U.S.C. § 2707—Damages

(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)

221. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

222. In relevant part, 18 U.S.C. § 2703 provides that:

> (a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
> (b) Contents of Wire or Electronic Communications in a Remote Computing Service.—
> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

223. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of the contents of Plaintiffs' communications while in electronic storage by an AT&T electronic communication service, and/or while carried or maintained by an AT&T remote computing service, in violation of 18 U.S.C. §§ 2703(a) and/or (b).

224. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' communications.

225. Defendants did not notify Plaintiffs of the disclosure of their communications, nor did Plaintiffs consent to such.

226. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and obtaining of disclosure of the contents of communications.

227. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2703, Plaintiffs seek from the Count XI Defendants for each Plaintiff their statutory damages or actual damages; punitive damages as appropriate; and such other and further relief as may be proper.

COUNT XII

Violation of 18 U.S.C. § 2703(a) & (b), actionable under 18 U.S.C. § 2712—Damages Against The United States

(Named Plaintiffs vs. Defendants United States, Department of Justice, and National Security Agency)

228. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

229. In relevant part, 18 U.S.C. § 2703 provides that:

> (a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
> (b) Contents of Wire or Electronic Communications in a Remote Computing Service.—
> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

230. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to the NSA of the contents of Plaintiffs' communications while in electronic storage by an AT&T electronic communication service, and/or while carried or maintained by an AT&T remote computing service, in violation of 18 U.S.C. §§ 2703(a) and/or (b).

231. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' communications.

232. Defendants did not notify Plaintiffs of the disclosure of their communications, nor did Plaintiffs consent to such.

233. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and obtaining of disclosure of the contents of communications.

234. Title 18 U.S.C. § 2712 provides a civil action against the United States and its agencies and departments for any person whose communications have been disclosed in willful

violation of 18 U.S.C. § 2703. Plaintiffs have complied fully with the claim presentment procedure of 18 U.S.C. § 2712. Pursuant to 18 U.S.C. § 2712, Plaintiffs seek from the Count XII Defendants for each Plaintiff their statutory damages or actual damages, and such other and further relief as is proper.

COUNT XIII

Violation of 18 U.S.C. § 2703(c)—Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

235. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

236. In relevant part, 18 U.S.C. § 2703(c) provides that:

> (c) Records Concerning Electronic Communication Service or Remote Computing Service.—
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
> (B) obtains a court order for such disclosure under subsection (d) of this section;
> (C) has the consent of the subscriber or customer to such disclosure;
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
> (E) seeks information under paragraph (2).
> (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;
> (D) length of service (including start date) and types of service utilized;

> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> (F) means and source of payment for such service (including any credit card or bank account number),
> of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
> (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

237. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' and class members' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c). In doing so, Defendants have acted in excess of their statutory authority and in violation of statutory limitations.

238. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' and class members' records or other information.

239. Defendants did not notify Plaintiffs or class members of the disclosure of these records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs or class members consent to such.

240. Plaintiffs and class members have been and are aggrieved by Defendants' above-described acts of soliciting and obtaining disclosure by AT&T of records or other information pertaining to Plaintiffs and class members.

241. On information and belief, the Count XIII Defendants are now engaging in and will continue to engage in the above-described soliciting and obtaining disclosure by AT&T of records or other information pertaining to Plaintiffs and class members, acting in excess of the Count XIII

Defendants' statutory authority and in violation of statutory limitations, including 18 U.S.C. § 2703(c), and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class members have no adequate remedy at law for the Count XIII Defendants' continuing unlawful conduct, and the Count XIII Defendants will continue to violate Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

242. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief against the Count XIII Defendants.

243. Plaintiffs seek that the Court declare that Defendants have violated their rights and the rights of the class; enjoin the Count XIII Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' statutory rights, including their rights under 18 U.S.C. § 2703; and award such other and further equitable relief as is proper.

COUNT XIV

Violation of 18 U.S.C. § 2703(c), actionable under 18 U.S.C. § 2707—Damages

(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)

244. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

245. In relevant part, 18 U.S.C. § 2703(c) provides that:

> (c) Records Concerning Electronic Communication Service or Remote Computing Service.—
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or

other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

246. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).

247. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' records or other information.

248. Defendants did not notify Plaintiffs of the disclosure of these records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs consent to such.

249. Plaintiffs have been and are aggrieved by Defendants' above-described acts of soliciting and obtaining disclosure by AT&T of records or other information pertaining to Plaintiffs.

250. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved by knowing or intentional violation of 18 U.S.C. § 2703, Plaintiffs seek from the Count XIV Defendants for each Plaintiff their statutory damages or actual damages; punitive damages as appropriate; and such other and further relief as may be proper.

COUNT XV

Violation of 18 U.S.C. § 2703(c), actionable under 18 U.S.C. § 2712—Damages Against The United States

(Named Plaintiffs vs. Defendants United States, Department of Justice, and National Security Agency)

251. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

252. In relevant part, 18 U.S.C. § 2703(c) provides that:

> (c) Records Concerning Electronic Communication Service or Remote Computing Service.—
> (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
> (B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;
(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;
(B) address;
(C) local and long distance telephone connection records, or records of session times and durations;
(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

253. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).

254. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' records or other information.

255. Defendants did not notify Plaintiffs of the disclosure of these records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs consent to such.

256. Plaintiffs have been and are aggrieved by Defendants' above-described acts of soliciting and obtaining disclosure by AT&T of records or other information pertaining to Plaintiffs.

257. Title 18 U.S.C. § 2712 provides a civil action against the United States and its agencies and departments for any person aggrieved by willful violation of 18 U.S.C. § 2703. Plaintiffs have complied fully with the claim presentment procedure of 18 U.S.C. § 2712. Pursuant to 18 U.S.C. § 2712, Plaintiffs seek from the Count XV Defendants for each Plaintiff their statutory damages or actual damages and such other and further relief as is proper.

COUNT XVI

Violation of the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.* - Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants United States, Department of Justice, National Security Agency, Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

258. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

259. The Program violates the Administrative Procedures Act, 5 U.S.C. § 701 *et seq.*, because Defendants' actions under the Program exceed statutory authority and limitations imposed by Congress through FISA, and through Chapters 119, 121 and 206 of Title 18 of the U.S. Code (the Wiretap Act, the Stored Communications Act, and the Pen Register Statute, respectively) and in violation of statutory rights under those laws; are not otherwise in accordance with law; are contrary to constitutional rights, including the Fourth Amendment, First Amendment, and separation of powers principles; and are taken without observance of procedures required by law.

260. Plaintiffs and class members are aggrieved by these violations because, as described previously in this Complaint, Defendants' actions under the Program has resulted in the interception, acquisition, disclosure, divulgence and/or use of the contents of their wire and electronic

communications, communications records, and other information in violation of their constitutional and statutory rights.

261. Plaintiffs seek nonmonetary relief against the Count XVI Defendants, including a declaration that Defendants have violated their rights and the rights of the class; an injunction enjoining the Count XVI Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' rights; and such other and further nonmonetary relief as is proper.

COUNT XVII

Violation of Separation of Powers - Declaratory, Injunctive, and Other Equitable Relief

(Named Plaintiffs and Class vs. Defendants United States, Department of Justice, National Security Agency, Bush (in his official and personal capacities), Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)

262. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

263. The Program violates the principles of separation of powers because it was authorized by the Executive in excess of the Executive's authority under Article II of the United States Constitution, in excess of statutory authority granted the Executive under FISA and under Chapters 119, 121 and 206 of Title 18 of the U.S. Code (the Wiretap Act, the Stored Communications Act, and the Pen Register Statute, respectively) and exceeds the statutory limits imposed on the Executive by Congress.

264. Plaintiffs and class members are aggrieved by these violations because, as described previously in this Complaint, Defendants' actions under the Program has resulted in the interception, acquisition, disclosure, divulgence and/or use of the contents of their wire and electronic communications, communications records, and other information in violation of their constitutional and statutory rights.

265. Plaintiffs seek nonmonetary relief against the Count XVII Defendants, including a declaration that Defendants have violated their rights and the rights of the class; an injunction enjoining the Count XVII Defendants, their agents, successors, and assigns, and all those in active concert and participation with them from violating the Plaintiffs' and class members' rights; and for such other and further nonmonetary relief as is proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court:

A. Declare that the Program as alleged herein violates without limitation Plaintiffs' and class members' rights under the First and Fourth Amendments to the Constitution; their statutory rights, including their rights under 18 U.S.C. § 2511, 18 U.S.C. § 2703, 50 US.C. § 1809, and the Administrative Procedures Act; and their rights under the constitutional principle of Separation of Powers.

B. Award Plaintiffs and the class equitable relief, including without limitation, a preliminary and permanent injunction pursuant to the First and Fourth Amendments to the United States Constitution prohibiting Defendants' continued use of the Program, and a preliminary and permanent injunction pursuant to the Fourth Amendment requiring Defendants to provide to Plaintiffs and the class an inventory of their communications, records, or other information that was seized in violation of the Fourth Amendment, and further requiring the destruction of all copies of those communications, records, or other information within the possession, custody, or control of Defendants.

C. Award Plaintiffs their statutory, actual, and punitive damages to the extent permitted by law and according to proof.

D. Award to Plaintiffs reasonable attorneys' fees and other costs of suit to the extent permitted by law.

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

//

//

JURY DEMAND

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: September 17, 2008

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (1455997)
LEE TIEN (148216)
KURT OPSAHL (191303)
KEVIN S. BANKSTON (217026)
JAMES S. TYRE (083117)
454 Shotwell Street
San Francisco, CA 94110
Telephone: 415/436-9333
415/436-9993 (fax)

RICHARD R. WIEBE (121156)
LAW OFFICE OF RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, CA 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

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

Attorneys for Plaintiffs