CASE NO. 19-16066
(PRIOR APPEALS: NOS. 10-15616, 15-16133)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (AS EXECUTRIX OF THE ESTATE OF GREGORY HICKS), 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. 6 of 8, Pages ER 844 to ER 1097

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

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKEY
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.)

VOLUME 1			
ECF No.	**Date**	**Document Description**	**Page**
464	4/25/19	Judgment	**ER 001**
463	4/25/19	Notice of Filing of Classified Order	**ER 002**
462	4/25/19	Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiffs' Cross-motion	**ER 003**
412	8/28/18	Order Regarding Discovery Dispute	**ER 029**
410	8/17/18	Order Requiring Dispositive Motions Briefing	**ER 031**
404	6/13/18	Order Denying Plaintiffs' Motion for Access to Classified Discovery Materials and Requiring Additional Briefing	**ER 034**
356	5/19/17	Minute Order	**ER 036**
347	3/21/17	Order Granting Joint Request for Case Management Conference	**ER 037**
340	2/19/16	Order Granting Motion to Lift Stay of Discovery	**ER 042**
321	2/10/15	Order Denying Plaintiffs' Motion for Partial Summary Judgment and Granting Defendants' Motion for Partial Summary Judgment	**ER 046**

153	7/23/13	Amended Order	**ER 056**
VOLUME 2			
ECF No.	**Date**	**Document Description**	**Page**
465	5/20/19	Plaintiffs' Notice of Appeal and Representation Statement	**ER 082**
432	11/2/18	Declaration of Edward J. Snowden	**ER 087**
		Exhibit 1/Exhibit A: NSA document "ST 09-0002 Working Draft, Office of The Inspector General, National Security Agency," March 24, 2009 ("NSA Draft OIG Report").	**ER 089**
431	11/2/18	Declaration of David E. McCraw	**ER 146**
VOLUME 3			
ECF No.	**Date**	**Document Description**	**Page**
417-2	9/28/18	September 28, 2018 Declaration of Cindy A. Cohn in Opposition to the Government's Motion for Summary Judgment	**ER 149**

		Exhibit A: Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014) ("PCLOB Section 215 Report").	**ER 151**
VOLUME 4			
ECF No.	**Date**	**Document Description**	**Page**
417-2	9/28/18	September 28, 2018 Declaration of Cindy A. Cohn in Opposition to the Government's Motion for Summary Judgment	**ER 390**
		Exhibit B: 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 Section 702 Report").	**ER 392**
VOLUME 5			
ECF No.	**Date**	**Document Description**	**Page**
417-3	9/28/18	September 28, 2018 Declaration of David A. Greene in Opposition to the Government's Motion for Summary Judgment (Exhibits D, E, F, G omitted)	**ER 589**

		Exhibit A: "PR/TT Order" issued by the Foreign Intelligence Surveillance Court compelling the bulk production of Internet metadata by electronic communications service providers.	**ER 592**
		Exhibit B: October 3, 2011 Order of the Foreign Intelligence Surveillance Court for the interception of Internet content.	**ER 710**
		Exhibit C: September 20, 2012 Opinion and Order of the Foreign Intelligence Surveillance Court.	**ER 796**
VOLUME 6			
ECF No.	**Date**	**Document Description**	**Page**
417-4	9/28/18	September 28, 2018 Declaration of Richard R. Wiebe in Opposition to the Government's Motion for Summary Judgment	**ER 844**
		Exhibit A: Primary Order in docket BR 10-10 issued by the Foreign Intelligence Surveillance Court compelling the bulk production of telephone call records by multiple telephone companies.	**ER 848**
		Exhibit B: Excerpt from NSA Inspector General compliance audit report that includes as Appendix C a letter filed with the FISC by the NSA (the "NSA Letter").	**ER 868**
		Exhibit C: AT&T's Transparency Report of January 2016.	**ER 908**

		Exhibit D: Verizon's Transparency Report for the first half of 2016.	**ER 921**
		Exhibit E: NSA document published by the New York Times and ProPublica on August 15, 2015.	**ER 930**
		Exhibit F: Excerpt from George Molczan, *A Legal And Law Enforcement Guide To Telephony* (2005).	**ER 932**
		Exhibit G: NSA document published by the New York Times and ProPublica on August 15, 2015.	**ER 943**
		Exhibit H: Exhibit A to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.	**ER 946**
		Exhibit I: Exhibit B to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.	**ER 953**
417-5	9/28/18	Declaration of Phillip Long	**ER 955**
417-6	9/28/18	Declaration of Dr. Brian Reid	**ER 960**
417-7	9/28/18	Declaration of Professor Matthew Blaze	**ER 979**
417-8	9/28/18	Declaration of Ashkan Soltani	**ER 993**
417-9	9/28/18	Declaration of Carolyn Jewel	**ER 999**
417-10	9/28/18	Declaration of Tash Hepting	**ER 1006**
417-11	9/28/18	Declaration of Young Boon Hicks	**ER 1012**
417-12	9/28/18	Declaration of Erik Knutzen	**ER 1014**

417-13	9/28/18	Declaration of Joice Walton	**ER 1019**
262	7/25/14	Declaration of Richard R. Wiebe in Support of Plaintiffs' Motion for Partial Summary Judgment, Exhibit E	**ER 1025**
89	7/2/12	Declaration of J. Scott Marcus (exhibits omitted)	**ER 1031**
85	7/2/12	Declaration of Mark Klein	**ER 1071**
		Exhibit A (redacted version)	**ER 1080**
		Exhibit B (redacted version)	**ER 1085**
		Exhibit C (redacted version)	**ER 1090**
VOLUME 7			
ECF No.	**Date**	**Document Description**	**Page**
1	9/18/08	Complaint	**ER 1098**
	8/21/19	District Court Docket Sheet in N.D. Cal. No. 08-CV-04373-JSW	**ER 1153**
VOLUME 8 – PROVISIONALLY UNDER SEAL			
ECF No.	**Date**	**Document Description**	**Page**
84-1	7/2/12	Declaration of James Russell (Exhibit A omitted)	**ER 1193**

84-2	7/2/12	Declaration of Mark Klein	**ER 1206**
84-3	7/2/12	**Exhibit A** (under seal unredacted version)	**ER 1216**
84-4	7/2/12	**Exhibit B** (under seal unredacted version)	**ER 1260**
84-5, 84-6	7/2/12	**Exhibit C** (under seal unredacted version)	**ER 1281**

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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 **September 28, 2018 Declaration Of RICHARD R. WIEBE In Opposition To The Government's Motion For Summary Judgment** 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 a Primary Order issued by the Foreign Intelligence Surveillance Court compelling the bulk production of telephone call records by multiple telephone companies. It was issued in FISC docket BR 10-10 ("BR" for "Business Records") and was declassified and publicly released by the Director of National Intelligence on his official website. *Available at* https://www.dni.gov/files/documents/11714/FISC Order, BR 10-10.pdf.

4. **Exhibit B:** Attached hereto as Exhibit B is a true and correct copy of an excerpt from an NSA Inspector General compliance audit report. The report includes as its Appendix C a letter filed with the FISC by the NSA reporting a non-compliance incident in the telephone call records program.

The letter filed with the FISC identifies in the caption to the letter the telecommunications companies that were compelled by Primary Order BR 10-10 to produce in bulk the telephone call records of their customers as AT&T, Verizon, Verizon Wireless, and Sprint. Ex. B at App. C (pp. 28-29 of Ex. B) ("In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications, Inc., and Cellco Partnership d/b/a Verizon Wireless, and Sprint . . . , Docket Number BR 10-10").

Exhibit B was released in response to a Freedom of Information Act lawsuit brought by the New York Times against the NSA, *see* Scheduling Order, *New York Times v. NSA*, ECF No. 10, No. 15-2383 (S.D.N.Y May 15, 2015). Exhibit B was declassified and publicly released by the NSA on August 11, 2015. *Available at* https://assets.documentcloud.org/documents/2271057/savage-nyt-foia-nsa-ig-fisa-br-reports.pdf.

Exhibit B was the subject of an article by the New York Times. *N.S.A. Used Phone Records Program to Seek Iran Operatives*, New York Times, Aug. 12, 2015, *available at* https://www.nytimes.com/2015/08/13/us/nsa-used-phone-records-program-to-seek-iran-operatives.html.

5. **Exhibit C:** Attached hereto as Exhibit C is a true and correct copy of AT&T's Transparency Report of January 2016. *Available at* https://about.att.com/content/dam/csr/Transparency Reports/ATT_Transparency Report_Jan 2016.pdf.

6. **Exhibit D:** Attached hereto as Exhibit D is a true and correct copy of Verizon's Transparency Report for the first half of 2016. *Available at* https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/07/Transparency-Report-US-1H-2016.pdf.

7. **Exhibit E:** Attached hereto as Exhibit E is a true and correct copy of an NSA document published by the New York Times and ProPublica on August 15, 2015. *Available at* https://assets.documentcloud.org/documents/2275521/nyt-propublica-fairview-stormbrew.pdf.

Article at: https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

and

https://www.nytimes.com/interactive/2015/08/15/us/documents.html.

8. **Exhibit F:** Attached hereto as Exhibit F is a true and correct copy of an excerpt from George Molczan, *A Legal And Law Enforcement Guide To Telephony* (2005).

9. **Exhibit G:** Attached hereto as Exhibit G is a true and correct copy of an NSA document published by the New York Times and ProPublica on August 15, 2015. *Available at* https://www.documentcloud.org/documents/2274320-sidtoday-fairview-and-stormbrew-live-on-the-net.html.

Article at: https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html

and

https://www.nytimes.com/interactive/2015/08/15/us/documents.html.

10. **Exhibit H:** Attached hereto as Exhibit H is a true and correct copy of Exhibit A to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.

11. **Exhibit I:** Attached hereto as Exhibit I is a true and correct copy of Exhibit B to Plaintiffs' Revised First Set of Requests for Admission, served June 19, 2017.

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 September 27, 2018.

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

EXHIBIT A

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE APPLICATION OF THE FEDERAL BUREAU OF INVESTIGATION FOR AN ORDER REQUIRING THE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR

10-10

PRIMARY ORDER

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

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

Derived from: Pleadings in the above-captioned docket
Declassify on: 19 February 2035

things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

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

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

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number BR 09-19 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below,

satisfies the requirements of the Act and, therefore,

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

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"[1] created by [redacted]

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

[1] For purposes of this Order "telephony metadata" includes comprehensive communications routing information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [redacted] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [redacted]

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

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

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein. Notwithstanding the requirements set forth below, Executive Branch and Legislative Branch personnel may be permitted

appropriate access to the BR metadata and certain information derived therefrom in order to facilitate their lawful oversight functions, which include, but are not limited to, those set forth below.

B. The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders. Access to the BR metadata for such purposes shall be limited to the NSA Collection Managers, Data Integrity Analysts, and System Administrators described in paragraph 16 of the Declaration of [redacted] Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency, filed as Exhibit A to the Application in the above-captioned docket ([redacted] Declaration"). Additional individuals directly involved in developing and testing technologies to be used with the BR metadata may be granted access to the BR metadata, provided such access is approved by NSA's Office of General Counsel (OGC) on a case-by-case basis. Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel, unless: (i) sharing is permitted under paragraph 3(J); or (ii) a data integrity analyst conducted the query using a RAS-approved

telephone identifier at the request of an analyst authorized to query the BR metadata pursuant to paragraph 3(C) below, or an analyst authorized to receive query results pursuant to paragraph 3(I) below.[2] Queries performed by the persons described in this paragraph shall not be subject to the approval process and standard set forth in paragraph (3)C below. To the extent NSA personnel make copies of the BR metadata for purposes of ensuring data integrity or developing and testing technological measures, such copies shall be destroyed upon the completion of their work.

C. Subject to the restrictions and procedures below, up to 125 NSA analysts may be authorized to access the BR metadata for purposes of obtaining foreign intelligence information through contact chaining [redacted] ("queries") using telephone identifiers,[3] as described in the [redacted] Declaration at paragraphs 8-13.

---

[2] The Court understands that only Data Integrity Analysts who have received the training required for access under paragraph 3(C) will be permitted to perform queries and share query results with analysts as described in (ii) above.

[redacted]

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

---

billing and/or routing communications, such as IMSI, IMEI, and calling card numbers.

[redacted]

[redacted]

provided, however, that NSA's OGC shall first determine that any telephone identifier reasonably believed to be

---

[redacted]

used by a United States (U.S.) person is not regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.[6]

(ii) Telephone identifiers that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by agents of [redacted]

[redacted]

[6] The Court understands that from time to time the information available to designated approving officials will indicate that a telephone identifier was, but may not presently be, or is, but was not formerly, associated with [redacted] In such a circumstance, so long as the designated approving official can determine that the reasonable, articulable suspicion standard can be met for a particular period of time with respect the telephone identifier, NSA may query the BR metadata using that telephone identifier. However, analysts conducting queries using such telephone identifiers must be made aware of the time period for which the telephone identifier has been associated with [redacted] in order that the analysis and

including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to telephone identifiers under surveillance pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a telephone identifier is associated with [redacted] shall be effective for: one hundred eighty days for U.S. telephone identifiers and for any identifiers believed to be used by a U.S. person; one year for all other telephone identifiers.[7]

---

minimization of the information retrieved from their queries may be informed by that fact.

[7] The Court understands that call detail records of foreign-to-foreign communications provided by [redacted] pursuant to this Order

D. The Director of the NSA shall continue to maintain mandatory procedures to strictly control access to and use of the BR metadata, in accordance with this Court's orders. NSA's OGC shall continue to promptly provide NSD with copies of these mandatory procedures (and all replacements, supplements or revisions thereto in effect now or adopted in the future). The Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate; Chief and Deputy Chief, Homeland Security Analysis Center; and the Homeland Mission Coordinators shall maintain appropriate management controls (e.g., records of all tasking decisions, audit and review procedures) for access to the metadata.

E. The NSA shall obtain the BR metadata from [redacted] via secure lines, and shall store and process the BR metadata on a secure internal network that NSA

---

will not be used to make chain summary records. Further, such records will be used solely for technical purposes, including use by NSA's data integrity analysts to correctly interpret and extract contact information in [redacted] international records. In the event that an NSA analyst performs an authorized query that includes a search of the BR metadata, and the results of that query include information from [redacted] foreign-to-foreign call detail records, NSA shall handle and minimize the information in those records in accordance with the minimization procedures in this Order, regardless of the authority pursuant to which NSA obtained the record. In contrast, if the analyst's query does not include a search of the BR metadata, and the results of that query include information from [redacted] foreign-to-foreign call

exclusively will operate.

F. Any processing by technical personnel of the BR metadata acquired pursuant to this order shall be conducted through the NSA's secure internal network, which shall be accessible only to authorized personnel, using accounts authorized by a user authentication service, based on user login and password.

G. Access to the metadata shall be controlled by user name and password. NSA's Oversight and Compliance Office shall monitor the designation of individuals with access to the BR metadata. When the BR metadata is accessed through queries under paragraphs (3)B or (3)C above, a software interface shall limit access to the BR metadata to authorized personnel, and the user's login, Internet Protocol (IP) address, date and time, and retrieval request shall be automatically logged for auditing capability.[8] When the BR metadata is accessed through any other means under paragraph (3)B above, the user's login, date and time shall be automatically logged for auditing capability.

---

detail records, then the minimization procedures in this Order shall not be applied to the information in those records.

[8] In addition, the Court understands from the Declaration of Lieutenant General Keith B. Alexander, Director of NSA (Ex. A to the Report of the United States filed in docket number BR 09-09 on August 17, 2009) that NSA has made a number of technical modifications that will prohibit analysts: a) from inadvertently accessing the BR metadata in [redacted]; b) from querying the BR metadata in [redacted] with non-RAS-approved identifiers; and c)

NSA's Office of Oversight and Compliance shall monitor the functioning of this automatic logging capability. All persons authorized for access to the BR metadata and other NSA personnel who are authorized to receive query results shall receive appropriate and adequate training concerning the authorization granted by this Order, the limited circumstances in which the BR metadata may be accessed, and/or other procedures and restrictions regarding the retrieval, storage, and dissemination of the metadata. NSA's OGC shall ensure that such training is provided.

H. NSA shall treat information from queries of the BR metadata in accordance with USSID 18 and shall apply USSID 18 to minimize and disseminate information concerning U.S. persons obtained from the records produced pursuant to the authorities granted herein. Additionally, before the NSA disseminates any U.S. person identifying information, the Chief of Information Sharing Services in the Signals Intelligence Directorate, the Senior Operations Officer at NSA's National Security Operations Center, the Signals Intelligence Directorate Director, the Deputy Director of the NSA, or the Director of the NSA must determine that the information identifying the U.S. person is in

---

from going beyond three "hops" from an identifier used to query the BR metadata in [redacted]

fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance. Notwithstanding the above requirements, NSA may share certain information, as appropriate, derived from the BR metadata, including U.S. person identifying information, with Executive Branch and Legislative Branch personnel in order to enable them to fulfill their lawful oversight functions, and, in the case of Executive Branch personnel, to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings. By 5:00 p.m. each Friday following the authorization requested herein, the government shall file a report listing each instance during the seven-day period ending the previous Friday in which NSA has shared, in any form, information obtained or derived from the BR metadata with anyone outside NSA. For each such instance, the government shall specify the date on which the information was shared, the recipient of the information, and the form in which the information was communicated (e.g., written report, e-mail, oral communication, etc.). For each such instance in which U.S. person information has been shared, except those involving Executive Branch personnel seeking to identify discoverable information, the Chief of Information Sharing Services in the

Signals Intelligence Directorate shall certify that one of the authorized officials identified above determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand the counterterrorism information or to assess its importance. This paragraph's reporting requirement is not intended to apply to instances in which BR metadata and information derived therefrom is shared with Executive Branch or Legislative Branch personnel in order to facilitate their lawful oversight functions.

I. Personnel authorized to query the BR metadata in paragraph (3)C above may use and share the results of authorized queries of the BR metadata among themselves and with NSA personnel, including those who are not authorized to access the BR metadata pursuant to paragraph (3)C, provided that all NSA personnel receiving such query results in any form (except for information properly disseminated outside NSA) shall first receive appropriate and adequate training and guidance regarding the rules and restrictions governing the use, storage, and dissemination of such information. NSA's Oversight and Compliance Office shall monitor the designation of individuals who have received the training and guidance necessary to receive the results of queries of the BR metadata.

J. Authorized personnel also may use and share the identity of high-volume telephone identifiers and [redacted] that they discover or have discovered as a result of access authorized under paragraphs (3)B and (3)C or as a result of technical personnel access under prior docket numbers in this matter, among themselves and with other NSA personnel, including those who are not authorized to access the BR metadata, for purposes of metadata reduction and management. The training requirements set forth in paragraph (3)I above for NSA personnel receiving query results shall not apply to personnel receiving such identifiers, which may have been identified through queries, so long as they are received solely for purposes of metadata reduction and management.

K. The BR metadata collected under this Court's Orders may be kept online (that is, accessible for queries) for five years from the date of acquisition, at which time it shall be destroyed.

L. At least twice before the expiration of the authorities granted herein, NSA's OGC shall conduct a random spot check, consisting of an examination of a sample of call detail records obtained, to ensure that NSA is receiving only data as authorized by the Court and not receiving the substantive content of communications.

M. At least twice before the expiration of the authorities granted herein, the Department of Justice's National Security Division (NSD) will review NSA's access to the BR metadata under paragraph (3)C above. Such reviews shall include a sample of the justifications designated approving officials relied upon to approve telephone identifiers for querying the BR metadata, and a review of the queries conducted.

N. NSA's OGC shall consult with NSD on all significant legal opinions that relate to the interpretation, scope, and/or implementation of the authorizations granted by the Court in this matter. When operationally practicable, such consultation shall occur in advance; otherwise, NSD shall be notified as soon as practicable.

O. NSA's OGC shall promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the

authorizations granted by this Order.

P. At least once before the expiration of the authorities granted herein, a meeting for the purpose of assessing compliance with this Court's orders in this matter shall be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's Signals Intelligence Directorate. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authorities granted herein.

Q. At least once before the expiration of the authorities granted herein, NSD shall meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter.

R. Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD, and the Court.

S. Within forty-five days of the issuance of this Order, NSA shall file a report with the Court describing the queries made since end of the reporting period of the last report filed pursuant to the Court's order in docket number BR 09-19. Additionally, any application to renew or reinstate the

authority granted herein shall include a report describing: (i) the queries made since the end of the reporting period of the last report filed with the Court; (ii) the manner in which NSA applied the procedures set forth in paragraph (3)C above; and (iii) any proposed changes in the way in which the call detail records would be received from the carriers and any significant changes to the systems NSA uses to receive, store, process, and disseminate BR metadata.

This authorization regarding [redacted] **and unknown persons in the United States and abroad affiliated with** [redacted] **and unknown persons in the United States and abroad affiliated with** [redacted] expires on the 21st day of May, 2010, at 5:00 p.m., Eastern Time.

Signed 02-26-2010 P03:36 PCP Eastern Time
Date Time

REGGIE B. WALTON
Judge, United States Foreign
Intelligence Surveillance Court

EXHIBIT B

U.S. Department of Justice

United States Attorney
Southern District of New York

86 Chambers Street
New York, New York 10007

August 11, 2015

By Electronic Mail

David E. McCraw, Esq.
Jeremy A. Kutner, Esq.
The New York Times Company
620 Eighth Avenue
New York, NY 10018
E-mail: mccrad@nytimes.com
jeremy.kutner@nytimes.com

Re: *The New York Times Co. and Charlie Savage v. National Security Agency*, 15 Civ. 2383 (KBF)

Dear David and Jeremy:

This Office represents the National Security Agency ("NSA"), the defendant in the above-referenced matter. Pursuant to the Scheduling Order, dated May 15, 2015, NSA has completed its review and processing of the attached documents. NSA is releasing 16 documents with redactions. Information has been redacted from these documents pursuant to 5 U.S.C. §§ 552(b)(1), (b)(3), and (b)(6). Each redacted document being released has been marked with the applicable FOIA exemption or exemptions.

If you have any questions, please do not hesitate to contact us.

Sincerely,

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

By: */s/ John Clopper*
JOHN D. CLOPPER
ANDREW E. KRAUSE
Assistant United States Attorneys
Telephone: (212) 637-2716/2769
Facsimile: (212) 637-0033
E-mail: john.clopper@usdoj.gov
andrew.krause@usdoj.gov

Enclosures

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL REPORT

~~(TS//SI//NF)~~ Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses

(ST-10-0004C)

29 September 2010

Derived From: NSA/CSS Classification Guide 1-52
Dated: 20070108
Declassify On: 20350712

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts audits, investigations, and inspections. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA/CSS activities are conducted in compliance with the law, executive orders, and regulations. The OIG also serves as ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether program objectives are being met and whether operations comply with law and regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests, complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) FIELD INSPECTIONS

(U) The inspection function consists of organizational and functional reviews undertaken as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with law and regulations. The Office of Field Inspections also partners with Inspectors General of the Service Cryptologic Elements to conduct joint inspections of consolidated cryptologic facilities.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

29 September 2010
IG-11201-10

TO: DISTRIBUTION

~~(TS//SI//NF)~~ SUBJECT: Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C) — ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our review of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records. We found that the delayed implementation of a new selector tracking application resulted in control weaknesses and the querying of an expired selector. Our review also identified a control weakness regarding data integrity functions. Management concurred with the findings and recommendations and has already completed one recommendation by implementing the new selector tracking application and verifying that controls are in place.

2. (U//~~FOUO~~) We incorporated management's comments in the report, where appropriate, and included the full text of management responses in Appendix D. As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General,* all recommendations and planned corrective actions are subject to follow-up until completion. Status reports should be directed to [redacted] Assistant Inspector General for Follow-up, at OPS 2B8076, Suite 6247, within 15 calendar days after target completion dates.

(b)(3)-P.L. 86-36

3. (U//~~FOUO~~) We appreciate the cooperation and courtesies extended to our personnel throughout the review. If you need additional information or clarification, please contact [redacted] on 963-2988s or by e-mail at [redacted]

George Ellard

GEORGE ELLARD
Inspector General

ST-10-0004C

(U/ /~~FOUO~~) DISTRIBUTION:
SV42
S2I4
S313
T132

cc:
DIRNSA
OGC
DOC (J. DeLong)
SID (W. Crumm)
S02
SV
S2
S2I
S3
S31
TD
T1
T12
T1222
T13
OGC IG POC
SID IG POC
TD IG POC

(b)(3)-P.L. 86-36

DOJ NSD

(b)(6)

IG
D/IG
D1/AIG for Follow-up
D11
D12
D13
D14

(U) TABLE OF CONTENTS

I. (U) EXECUTIVE SUMMARY v

II. (U) BACKGROUND 1

~~(TS//SI//NF)~~ Terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) 1

~~(TS//SI//NF)~~ Testing of Compliance with the BR Order 1

III. (U) FINDINGS 3

(U//~~FOUO)~~ Expired Selector Was Queried 3

(U//~~FOUO)~~ Controls Are Not in Place 4

(U//~~FOUO)~~ Analysts' Duties Are Not Clearly Defined and Separated 5

IV. (U) ACRONYMS AND ORGANIZATIONS 7

APPENDIX A: (U) Objective, Scope, and Methodology

APPENDIX B: (U) Summary of Recommendations

APPENDIX C: ~~(TS//SI//NF)~~ DoJ Letter to FISC Regarding Incident Involving the BR Order

APPENDIX D: (U) Full Text of Management Response

(U) This page intentionally left blank.

~~(TS//SI//NF)~~ Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses

I. (U) EXECUTIVE SUMMARY

(U) OVERVIEW

~~(TS//SI//NF)~~ In May 2010, the Office of the Inspector General issued a Pilot Test Report (IG-111545-10) as part of our ongoing audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR) (ST-10-0004). In the report, we identified three control weaknesses in querying BR metadata. We did not make formal recommendations because the release of [redacted] a new selector tracking application that would address those weaknesses, was believed to be imminent—first in April 2010 and then in May 2010. However, because [redacted] release date kept slipping (it was released on 25 June 2010) and because a March 2010 query of an expired selector underscored one of those reported control weaknesses and identified an additional weakness regarding data integrity functions, we recommended that Agency management take immediate action.

(b)(3)-P.L. 86-36

(U) HIGHLIGHTS

~~(TS//SI//NF)~~ While testing March 2010 data, we found that an expired selector marked as approved was queried by a Data Integrity Analyst (DIA) for what seemed to be foreign intelligence purposes. The Department of Justice reported the query as an incident of non-compliance in August 2010; however, NSA disagreed that the query constituted a violation because the reasonable articulable suspicion approval was valid for the time-bounded period queried. Regardless, the query raised the following concerns:

- ~~(C//REL TO USA, FVEY)~~ A DIA was able to query an expired selector because controls were not in place to prevent such queries and the manual process that management had temporarily put in place did not identify the selector as needing revalidation.

- ~~(TS//SI//NF)~~ DIAs can query BR metadata for both data integrity and foreign intelligence purposes, increasing the risk for non-compliance with the Order.

~~(TS//SI//NF)~~ Management concurred with the recommendations in our audit report and completed one. Specifically, management released [redacted] in June 2010 and has verified that controls are now in place to address selector revalidations and the two remaining control weaknesses that we reported in the Pilot Test Report.

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

II. (U) BACKGROUND

~~(TS//SI//NF)~~ Terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR)

~~(TS//SI//NF)~~ The FISC BR Order requires that U.S. selectors be revalidated every 180 days and that all other selectors be revalidated every year. Data Integrity Analysts (DIAs) can query any selector, regardless of its approval status, for data integrity purposes. However, DIAs are prohibited from querying expired selectors (i.e., selectors not revalidated within the mandated timeframe) for foreign intelligence purposes. A Department of Justice (DoJ) National Security Division representative stated that a query made by a DIA to provide direct assistance to a foreign intelligence analyst constitutes querying for foreign intelligence purposes because the query results are shared with the analyst for intelligence analysis.

~~(C//REL TO USA, FVEY)~~ To meet the querying terms of the BR Order, NSA implemented standard operating procedures requiring DIAs to operate within the same control structure as foreign intelligence analysts when providing direct assistance. Specifically, these procedures require that DIAs use the standard login, which prevents such violations as querying selectors that are not approved when "reviewing telephone identifiers prior to and or after the issuance of a serialized report," and "[helping] analysts interpret and understand the results of their queries." When DIAs conduct data integrity analysis, procedures require that they use a special login that bypasses such controls. The procedures specify that DIAs should not use the bypass login when providing direct assistance to foreign intelligence analysts.

~~(TS//SI//NF)~~ Testing of Compliance with the BR Order

~~(TS//SI//NF)~~ We began our review by pilot testing compliance with six requirements of the BR Order relating to querying and dissemination. The goal was to ensure that each requirement was testable using the continuous auditing method. To determine whether controls are operating as intended, we are continuing our review with monthly testing of NSA compliance with seven requirements of the BR Order for 2010. To date, we have completed testing and reported results of data from January through July 2010.

(U) This page intentionally left blank.

III. (U) FINDINGS

~~(TS//SI//NF)~~ *During our monthly testing of March 2010 data, we found that a U.S. selector had not been revalidated at 180 days, as mandated by the BR Order, and the selector remained "approved" for querying in the BR Foreign Intelligence Surveillance Act (FISA) database for 16 days past the expiration date. As a result, a DIA was able to query that selector, in possible violation of the Order. This incident occurred because adequate controls were not in place to revalidate reasonable articulable suspicion (RAS) determinations of selectors, as mandated by the Order. We reported this weakness, along with two others, in our Pilot Test Report. The incident also revealed an additional control weakness: DIAs can query BR metadata for both data integrity and foreign intelligence purposes, increasing the risk for non-compliance.*

(U//~~FOUO~~) Expired Selector Was Queried

(b)(3)-P.L. 86-36
(b)(3)-18 USC 798

~~(C//REL TO USA, FVEY)~~ While testing March 2010 data, we found that an expired selector marked as approved had been queried by a DIA for what seemed to be foreign intelligence purposes. The U.S. person selector had been approved [redacted] but had not been revalidated on its expiration date, [redacted] The selector was still marked as approved [redacted] when, in response to a customer request for information associated with 2009 reporting, a DIA queried the selector [redacted] The DIA followed standard operating procedures for providing direct assistance by using a standard login rather than bypassing querying controls and did not indicate in the justification field that the query was for data integrity purposes. The selector was changed to "not approved" [redacted] 16 days after its expiration. No other queries of this selector had been made.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//REL TO USA, FVEY)~~ Because the query seemed to have been conducted for foreign intelligence purposes, we notified management of the possible non-compliance incident, and Special FISA Oversight and Processing (SV42) issued an incident report on 25 May 2010. On 2 August 2010, the DoJ National Security Division reported the query as a compliance incident pursuant to Rule 10(c) of the FISC Rules of Procedure, effective 17 February 2006 (see Appendix C). However, NSA disagreed with DoJ that the query constituted a violation of the Order because the RAS approval was valid for the time-bounded period queried by the DIA to answer the client's technical question. NSA's position is described in detail in Appendix D.

(U//~~FOUO~~) Controls Were Not in Place

~~(C//REL TO USA, FVEY)~~ A DIA was able to query an expired selector because controls were not in place to prevent such queries and the manual process that management had temporarily put in place did not identify this selector as needing revalidation. This weakness, along with two others, was identified in our Pilot Test Report. We did not make recommendations at that time because we found no incidents of non-compliance and the control weaknesses were to be resolved with the release of [redacted] a new selector tracking application, then planned for May 2010.

(b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ Because [redacted] release date kept slipping, the risk for non-compliance remained for requirements related to U.S. persons, selector revalidations, and time-restricted selectors. However, Agency management reported on 28 June 2010 that [redacted] had been released on 25 June 2010 and was operational.

(U) RECOMMENDATION 1

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are functioning to:

a. prevent querying selectors associated with U.S. persons without a documented Office of General Counsel review for First Amendment considerations;

b. prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively); and

c. tag, track, and identify time-restricted selectors.

(U) (ACTION: Homeland Security Analysis Center [S2I4] with SV42)

(b)(3)-P.L. 86-36

(U) Management Response

(U//~~FOUO~~) **CONCUR.** Management concurred with the finding and recommendation and has taken appropriate action. [redacted] was implemented on 25 June 2010, and the Director of Compliance, Office of General Counsel, SID Oversight and Compliance, and DoJ representatives were provided demonstrations and expressed their approval.

(U) OIG Comment

(U//~~FOUO~~) Management has taken corrective action that meets the intent of the recommendation.

(U//~~FOUO~~) Analysts' Duties Are Not Clearly Defined and Separated

~~(C//REL TO USA, FVEY)~~ The March 2010 query of an expired selector revealed another weakness: DIAs can query selectors for data integrity and foreign intelligence purposes. The *Standards for Internal Control in the Federal Government* state that key duties and responsibilities should be divided among different people to reduce the risk for error and fraud. No one individual should control all key aspects of transactions or events. Although DIAs do not conduct target analysis or report on targets, they might help a foreign intelligence analyst with a question on a target. In those cases, the DIA is querying for foreign intelligence purposes, not data integrity, and must use the same rules as foreign intelligence analysts. These procedures require that DIAs and foreign intelligence analysts use a standard login that invokes controls over querying, such as preventing the querying of selectors with a status of "not approved." However, DIAs also use special logins that bypass such controls and allow them, for example, to query selectors that are not approved, which is permitted for data integrity analysis but puts DIAs at risk for querying for foreign intelligence purposes without controls.

~~(C//REL TO USA, FVEY)~~ The March 2010 incident revealed that the functions of DIAs are not clearly defined and communicated. It is unclear whether the DIA's query was for data integrity or foreign intelligence purposes. The standards for internal control require that key areas of authority and responsibility be defined and communicated throughout the organization. The standards also call for managers to document clearly such internal control mechanisms in management directives, administrative policies, or operating manuals that are readily available.

~~(TS//SI//NF)~~ Although S2I4 management stated that they discussed with DoJ the appropriate functions of DIAs, personnel did not have a common understanding of the types of queries appropriate for foreign intelligence and data integrity purposes. Furthermore, existing guidance did not clearly link the types of queries with the purpose of querying, and supplementary guidance was still in draft. For example, after we identified that an expired selector had been queried in March 2010, it was unclear whether the query had violated the FISC BR Order. Specifically, personnel had differences of opinion as to whether the query had been for foreign intelligence purposes and, therefore, a violation or for data integrity purposes, which is not a violation.

~~(TS//SI//NF)~~ Without clearly defined roles, a distinct separation of duties, and well-understood policies that differentiate queries for foreign intelligence and data integrity purposes, DIAs are vulnerable to errors

and violations of the FISC BR Order. In particular, DIAs might mistakenly query selectors for foreign intelligence purposes while using the special login that bypasses key controls.

(U) RECOMMENDATION 2

~~(TS//SI//NF)~~ Clearly define and separate the duties of DIAs and foreign intelligence analysts. Specifically, implement controls to prevent an individual from querying BR metadata for both data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.

(U) (ACTION: Exploitation Solutions Office [S313] and Structured Repositories [T132])

(U) Management Response

(U//~~FOUO~~) **CONCUR.** Management concurred with the finding and recommendation and provided target completion dates. Management plans to move data integrity functions out of S2I4 and into S313, and T132 and will develop appropriate procedures and job descriptions.

(U) OIG Comment

(U//~~FOUO~~) Planned and ongoing actions meet the intent of our recommendation.

IV. (U) ACRONYMS AND ORGANIZATIONS

~~(TS//SI//NF)~~ BR	Business Records
(U) DIA	Data Integrity Analyst
(U) DoJ	Department of Justice
(U) FISA	Foreign Intelligence Surveillance Act
(U) FISC	Foreign Intelligence Surveillance Court
(U) RAS	reasonable articulable suspicion
(U) S2I4	Homeland Security Analysis Center
(U) S313	Exploitation Solutions Office
(U) SV42	Special FISA Oversight and Processing
(U) T132	Structured Repositories

(U) This page intentionally left blank.

(U) APPENDIX A

(U) Objective, Scope, and Methodology

(U) This page intentionally left blank.

ST-10-0004C

(U) ABOUT THE AUDIT

(U) Objective, Scope, and Methodology

(U) Objective

~~(TS//SI//NF)~~ The overall objective of this audit is to test whether controls to ensure NSA compliance with key terms of the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) are operating as intended. During the pilot test phase of the audit, our objective was to determine NSA compliance and assess the feasibility and reasonableness of including in monthly testing six objectives related to querying and dissemination. For monthly testing, our objective is to test NSA's compliance with seven requirements of the BR Order and determine whether controls are operating as intended.

(U) Scope and Methodology

(U) We conducted pilot testing from January to March 2010; monthly testing of January through July 2010 data was conducted from March to August 2010.

~~(TS//SI//NF)~~ For both pilot testing and monthly testing, we compared all selectors that were documented in [redacted] audit logs and had been queried each month against access lists, reasonable articulable suspicion approvals documented in the Foreign Intelligence Surveillance Act BR database, and Office of General Counsel reviews documented in the Homeland Requests Database. We also counted the number of hops chained for each selector in the [redacted] audit logs. For monthly testing, we also applied these tests to queries of the [redacted] We researched any anomalies to make a final determination of compliance.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) We met with individuals from the Office of General Counsel (OGC), the SIGINT Directorate, and the Technology Directorate, including the SID Office of Oversight and Compliance, Information Sharing Services, Homeland Security Analysis Center, SID Issues Support Staff, Analytic Capabilities, Structured Repositories, and [redacted] Operations.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Details on the scope and methodology used for pilot testing, including scope limitations, are included in our Pilot Test Report (IG-11154-10). Details on monthly testing are included in the January to March 2010 Test Report (IG-11160-10), April 2010 Test Report (IG-11163-10), May 2010 Test Report (IG-11174-10), June 2010 Test Report (IG-11179-10), and July 2010 Test Report (IG-11188-10).

(U) We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions according to our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions according to our audit objectives.

(U) APPENDIX B

(U) Summary of Recommendations

(U) This page intentionally left blank.

ST-10-0004C

(U) Summary of Recommendations

Recommendation 1

~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are in place and functioning to:

(b)(3)-P.L. 86-36

a. prevent querying selectors associated with U.S. persons without a documented OGC review for First Amendment considerations;

b. prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively); and

c. tag, track, and identify time-restricted selectors.

(U) Status: CLOSED

Recommendation 2

~~(TS//SI//NF)~~ Clearly define and separate the duties of data integrity analysts and foreign intelligence analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes, and issue formal guidance to differentiate such queries (ACTION: Exploitation Solutions Office [S313] and T132).

(U) Status: OPEN
(U) Target Completion Dates: [redacted] for S313 for T132

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX C

~~(TS//SI//NF)~~ DoJ Letter to FISC Regarding Incident Involving the BR Order

(U) This page intentionally left blank.

U.S. Department of Justice

National Security Division

2010 AUG -2 PM 4:32

TOP SECRET//COMINT//NOFORN

Washington, D.C. 20530

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
U.S. Courthouse
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Compliance Incident Involving In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from AT&T, the Operating Subsidiaries of Verizon Communications Inc., and Cellco Partnership d/b/a Verizon Wireless, and Sprint Relating to al Qaeda and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with al Qaeda and Associated Terrorist Organizations and the Government of Iran and Associated Terrorist Organizations and Unknown Persons in the United States and Abroad Affiliated with the Government of Iran and Associated Terrorist Organizations, Docket Number BR 10-10 (TS)

Dear Judge Bates:

Pursuant to Rule 10(c) of the Foreign Intelligence Surveillance Court (FISC) Rules of Procedure, effective February 17, 2006, this letter further advises the Court of a compliance incident regarding docket number BR 10-10. A preliminary notice regarding the incident was filed with the Court on July 26, 2010. (S)

On February 26, 2010, in docket number BR 10-10, Judge Reggie B. Walton approved an application for tangible things. Judge Walton renewed that authority on May 14, 2010, in docket number BR 10-17, expiring on August 6, 2010. The Court's Primary Order in docket number BR 10-10 states: "The BR metadata may be accessed for the purposes of ensuring data integrity and developing and testing any technological measures designed to enable the NSA to comply with the Court's orders." Docket Number BR 10-10, Primary Order at 5. "Persons who query the BR metadata pursuant to this paragraph may only share the results of any such query with other specially-cleared NSA technical personnel," with limited exceptions, including when "a data integrity analyst [DIA] conduct[s] the query using a RAS-approved telephone identifier at the request of an analyst authorized to query the BR metadata" *Id.* at 5-6. (TS//SI//NF)

On July 16, 2010, the National Security Agency (NSA) advised the Department of Justice's National Security Division of the compliance incident described below:

TOP SECRET//COMINT//NOFORN

Classified by: David S. Kris, Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 2 August 2035

- On March 9, 2010, a DIA queried the BR metadata in response to a Federal Bureau of Investigation (FBI) request for certain information relating to a United States telephone identifier referenced in a previously issued NSA report. Specifically, the FBI inquired whether the BR metadata contained information indicating that the identifier was roaming during in the [redacted] to [redacted] time frame. (TS//SI//NF)
- The reasonable, articulable suspicion (RAS) approval for the identifier expired on [redacted], [redacted], [redacted] before the query. (It had been RAS-approved on [redacted], [redacted].) Still, the identifier was listed on the Station Table – historically, NSA's list of identifiers that have undergone RAS determinations – as RAS-approved until [redacted], [redacted] at which time its status was changed to "not approved." (TS//SI//NF)
- The DIA used the identifier to conduct a single query of the BR metadata in the Transaction Database. Although the preliminary notice of this incident reported that the query was time-bounded to the period of [redacted] through [redacted], the query was not time-bounded. Rather, the DIA focused his review of the query results to the time period referenced in the FBI's request for information. (TS//SI//NF)
- Based on the query results, the DIA determined that no roaming data was available for the identifier, and NSA provided that information to the FBI. NSA did not issue a report based on this query. (TS//SI//NF)

This incident was discovered by the staff of NSA's Inspector General through their review of controls used to comply with the Court's Orders in this matter. NSA confirms that it conducted no queries using the identifier after the DIA's query described above. (TS//SI//NF)

At the time of this incident, NSA managed the RAS-approval status of identifiers on the Station Table through a periodic, manual review of those identifiers. NSA assesses that this compliance incident resulted from delays in the manual review process. NSA further assesses that a technical modification likely will prevent this sort of compliance incident from occurring in the future. In June 2010, NSA implemented a new program to manage and track requests to approve the use of identifiers that meet the RAS standard. This new program, among other things, automatically changes an identifier's status to "not approved" if it has not been re-approved for RAS within the time frame specified by the Court's orders. (TS//SI//NF)

[redacted], Global Capabilities Manager, Counterterrorism, reviewed a draft of this letter and confirmed its accuracy. (U)

Sincerely,

[redacted]
Section Chief, Oversight
National Security Division
U.S. Department of Justice

cc: The Honorable Reggie B. Walton

(U) APPENDIX D

(U) Full Text of Management Response

(U) This page intentionally left blank.

~~TOP SECRET//COMINT//NOFORN~~ DOCID: 4230249 REF ID:A4197247

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
OIG	2010-4645	

THRU	ACTION	EXREG SUSPENSE
	☐ APPROVAL	18 Aug 2010
SUBJECT: ~~(TS//SI//NF)~~ SID Response: Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)	☐ SIGNATURE	KCC SUSPENSE
	X INFORMATION	ELEMENT SUSPENSE: 2 Aug 2010

DISTRIBUTION
SID, S02, S2, SV, D4, T12, OGC

SUMMARY

PURPOSE: ~~(TS//SI//NF)~~ To provide the SID Response to the subject DRAFT Report.

BACKGROUND: ~~(TS//SI//NF)~~ In May 2010, the OIG issued the Pilot Test Report (IG-11154-10) as part of the ongoing audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records (BR) (ST-10-0004). The pilot testing identified three control weaknesses in querying BR metadata as well as concerns related to the dissemination of information. Because there was no evidence of non-compliance and the release of the new selector tracking application that would address the weaknesses [redacted] was imminent, the OIG didn't make formal recommendations opting to monitor the situation and make formal recommendations as necessary.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ The continual slippage of [redacted] release date [redacted] released June 25, 2010) coupled with the March 2010 non-compliance incident (which underscored one of the reported control weaknesses and identified an additional weakness) resulted in the OIG recommending Agency management take immediate action. The subject quick-reaction draft report is the result of the problem that warranted immediate attention by Agency Management.

DISCUSSION: ~~(TS//SI//NF)~~ The SID Response to the subject document has been coordinated with S2, SV, T12, D4 and OGC. It includes the response to the two Recommendations for SID Lead and NSA's response to the DOJ's notice of violation. Also included for your reference is the SV42 response to the March 2010 incident relative to the subject report.

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
for SID DIR	[redacted] 8-20-2010	963-7400	D4	John DeLong//email//8/6/10	
S02	[redacted] 8/19/10		OGC	[redacted]//email//8/9/10	963-8309
S2	[redacted]//s//3 Aug 10	963-3335	S3	[redacted]	
SV	[redacted]//email//2 Aug 10	963-1705		[redacted]	
T12	[redacted]//email//8/6/10	963-0247			

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
SID IG Liaison, [redacted]	S023	966-5590	11 August 2010

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

FORM A6796

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

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

~~(TS//SI//NF)~~ SID Response: Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

~~(TS//SI//NF)~~ **Introduction**: The SID Response has been coordinated with the Deputy Directorate for Analysis and Production (S2), SID Oversight and Compliance (SV), and the Office of General Counsel (OGC) because the same issue is being addressed in parallel channels at the SID level and above. The Department of Justice (DOJ) filed a 10c notice of violation with the Foreign Intelligence Surveillance Court (FISC) to which NSA, through OGC, is providing a non-concurrence on describing this event as a violation. NSA's response to DOJ is included in the Background and Context section of this document. It is being provided to ensure that NSA provides consistent responses and appropriate context to these parallel reporting actions. While NSA does not agree that this event was clearly an 'incident of non-compliance,' it does highlight deficiencies in the previous selector management application; nevertheless it falls short of a compliance violation.

(b)(3)-P.L. 86-36

RECOMMENDATION 1: ~~(TS//SI//NF)~~ Immediately verify that controls in the newly released version of [redacted] are in place and functioning to:

a) prevent querying selectors associated with U.S. persons without a documented OGC review for First Amendment considerations,

b) prevent querying selectors not revalidated within BR-mandated limits (180 days and one year for U.S. and foreign selectors, respectively), and

c) tag, track, and identify time-restricted selectors.

If the conditions in a, b, and c cannot be verified, immediately develop and implement interim plans to address these weaknesses until [redacted] can be modified.

SID Action Element: Chief, S2I4 with SV42 and T1222

SID RESPONSE (August 2010): (U//~~FOUO~~) SID concurs with this recommendation. On 25 June 2010 the new selector management system, [redacted] was activated and all deficiencies noted in the OIG report have been addressed. The OIG has been provided real time updates associated with this release and has interacted with S2I4's [redacted] liaison in order to perform their own review of the application. Additionally, the Office of the Director of Compliance (ODoC), Office of General Counsel (OGC), SID Oversight and Compliance (SV), Office of the Inspector General (OIG) and Department of Justice representatives have all had [redacted] functionalities demonstrated to them and expressed their approval (see additional information in Explanatory Remarks section)

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224

(b)(3)-P.L. 86-36

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

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

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

~~(TS//SI//NF)~~ Quick-Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

~~(TS//SI//NF)~~ March 2010 Non-Compliance Incident – Additional Information

~~(TS//SI//NF)~~ SID Oversight and Compliance/FISA Authorities (SV4) emphasizes that all of the items listed in recommendation 1 are procedures and features of the [redacted] program that have been in place since June 28, 2010. NSA Way [redacted] initial operating capability was concluded by T12 personnel on June 22, 2010. This acceptance should serve as the testing verification for the requirements set out in recommendation 1 of the subject report.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Operational testing and evaluation is on-going under real-world use while the developers and technical oversight personnel are monitoring "bug reports" and user feedback with a keen eye toward compliance issues. In addition, an Emergency Change process is established with a cross-organization technical and oversight team in place to resolve any compliance findings or to determine adjustments to the program should changes in the legal environment occur.

(U) SV42 proposal related to Recommendation 2.

~~(TS//SI//NF)~~ Below are the DIA roles and specific functions as defined in the Data Integrity Analyst [redacted] Standard Operating Procedures (SOP), dated September 28, 2009, while the DIA's were assigned to the SIGINT Directorate.

~~(TS//SI//NF)~~ In the SOP, the DIA's have three tools or roles within [redacted] to perform their functions: (b)(3)-P.L. 86-36

A. The first role [redacted] and was described as only for the use of providing support to analysts both in and out of the CT product line.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

B. The second available role [redacted] Within this second role was a list of typical support:

1. Reviewing telephone identifiers prior to and or after the issuance of a serialized report or a Request for Information (RFI) in order to verify the accuracy of the [redacted] data. (b)(3)-P.L. 86-36
2. Helping analysts interpret and understand the results of their queries.
3. Confirm [redacted]

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

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

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

C. The third role [redacted] which provides the DIA by-pass capability. This third tool was described for use in technical and data integrity purposes only and the by-pass capability was specifically called out not to be used to support functions in sections A. or B above.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ SV4 recommends that those offices that have taken on the functions, previously or currently known as the Data Integrity Analysts, establish a policy that clearly defines and prohibits the use of RAS by-pass modes while working on data for or assisting other analysts for intelligence analysis purposes.

~~(TS//SI//NF)~~ The policy should state that the use of any RAS by-pass functions should be limited to processing and data formatting purposes to ensure that the metadata is accurate and usable by analysts and to ensure compliance with the FISA Court Orders.

~~(TS//SI//NF)~~ The policy should allow that technical support personnel or DNR Subject Matter Experts working with BR FISA metadata should be able to continue to provide *technical* support to intelligence analysts for the purposes of assistance with accuracy and technical interpretation of the metadata with or without any RAS by-pass function enabled.

~~(TS//SI//NF)~~ However, the policy should strictly prohibit the use of a RAS by-pass function by technical support personnel or DNR Subject Matter Experts as described above to assist with or provide any analytic interpretation of results of queries against the BR FISA database that would supply any information of intelligence value.

POC: [redacted] SV42, 969-0024
Approved by: [redacted] *Chief SID Oversight and Compliance, 2 August 2010*

(b)(3)-P.L. 86-36

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

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

RECOMMENDATION 2: ~~(TS//SI//NF)~~ Clearly define and separate the duties of Data Integrity Analysts and Foreign Intelligence Analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.

(U) (ACTION: Chief, S2I4 with SV42 and T1222)

SID RESPONSE (August 2010): ~~(TS//SI//NF)~~ SID does not concur that this is an action for Chief, Homeland Security Analysis (S2I4) as stated in the recommendation. Counterterrorism (CT) Production Center (S2I) does not intend to retain individuals in a 'data integrity analyst' (DIA) capacity and is working to transition those functions to where they fit better within SID. The DIA function is one of the legacy constructs tracing back to a former NSA compartmented program. The DIA's role was not clearly distinct from target analysts. S2I4 determined during the end-to-end reviews that data integrity analyst functions should be moved out of the production organization and aligned with other corporate elements within SID's SIGDEV Strategy and Governance (SSG) and Deputy Directorate for Data Acquisition (S3), who perform similar functions related to data integrity and fidelity at the point of ingest. Transition of DIA functions, not DIA positions, is ongoing with Cryptanalysis and Exploitation Services (CES) (S31)/Exploitation Solutions Office (ESO)(S313) and SSG. S2I has been working with Chief, Protocol Exploitations (S31323) on this transition of functions. S2I4 leadership has asked TD to relocate the single remaining DIA (a TD resource) to T spaces. The analyst who performed the March 2010 query recently took a new job in SSG.

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224
POC: [redacted] Chief S313, Exploitation Solutions Office, [redacted] 963-3101

(U) Background and Context:

(b)(3)-P.L. 86-36

~~(C//REL TO USA, FVEY)~~ Where S2I4 diverges from this report as written is in the description of the query performed in March 2010 as an 'Incident of Non-Compliance'. The report fails to provide adequate background context.

~~(TS//SI//NF)~~ The following was provided to OGC and DOJ for review as an explanation of the chain of events in the course of DOJ filing an initial 10c:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

[redacted]

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

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

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ S2I4 has no contention that the query performed [redacted] and noted in an OIG audit highlighted specific deficiencies in the legacy applications used to manage RAS approved selectors. These same findings were noted during the End-to-End reviews of both the Business Records and Pen Register Trap & Trace FISA programs. S2I4 leadership strongly agreed with the recommendation to delay the release of the [redacted] application until such time as: 1) the End-to-End review findings were complete and had been fully discussed with DOJ and 2) those findings could be incorporated into [redacted] to address compliance vulnerabilities.

(b)(3)-P.L. 86-36

~~(S//NF)~~ A new revalidation process was established and implemented in the fall of 2009, albeit a completely manual process as [redacted] was being re-engineered. Prior to [redacted] release each program had a separate and distinct [redacted] underpinned by its own application, leaving NSA with a purely manual process during this transition. S2I4 and TD counterparts validated all previous 'customer requirements' for [redacted] and worked through the 'NSA Way' process to completion. SV and OGC are also 'customers' of this application and along with ODoC, had visibility into the entire revamping process. This engagement continues to address any issues noted after [redacted] release.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ Nonetheless, the legacy system's deficiency allowed a DIA to query on a selector that should have no longer been retained in [redacted] as RAS approved. [redacted] It should be noted however, the DIA could still have queried on that selector [redacted] as part of their 'data integrity' duties --- within the bounds of the order and without RAS approval.

(U//~~FOUO~~) Explanatory Remarks related to Recommendation 1:

a) ~~(S//NF)~~ Any selector being reviewed for RAS that is a US identifier or is believed to be in use by a US person cannot be RAS approved without an OGC First Amendment review. As the nomination is entered into [redacted] a field to note whether the selector is foreign or domestic must be populated for the nomination to be processed. When the domestic field is populated, [redacted] sends the nomination to OGC for review and no further action can be taken until that review is completed.

(b)(3)-P.L. 86-36

b) ~~(TS//SI//NF)~~ As a selector is approved within the [redacted] selector management system, a revalidation date is set tied to the date of approval

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

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

and whether it is US or foreign. HSAC [Homeland Security Advisory Council] internal management guidelines are that all US selectors will be revalidated every 90 days and foreign selectors at 180 days. This protocol should preclude any instance of exceeding FISC mandated timeframes. [redacted] will automatically move these selectors into a pending status 15 days from the projected 'expiration'. If any selector in this status has not been revalidated by the cut-off date, [redacted] moves the selector into an expired state. The selector is no longer noted as 'RAS approved' in the system [redacted] and [redacted] is informed of this action in order to ensure this selector can no longer be queried in the [redacted] BRF or PR/TT repositories.

(b)(3)-P.L. 86-36

c) ~~(C//REL TO USA, FVEY)~~ 'Time Bounded Query' restrictions have their own icon which prompts an analyst to check a selector's record within the [redacted] system. This record notates the time restriction and informs analysts of the specific timeframe they must focus on during the review of query results. Information outside of those boundaries must not be used in the pursuit of their targets. [redacted]

POC: [redacted] Chief, S2I4, CT Homeland Security Analysis, [redacted] 969-0224
Approved by: DDAP, [redacted] 3 Aug 10

(b)(3)-P.L. 86-36

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

Quick Reaction Draft Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – Control Weaknesses (ST-10-0004C)

RECOMMENDATION 2: ~~(TS//SI//NF)~~ Clearly define and separate the duties of Data Integrity Analysts (DIA) and Foreign Intelligence Analysts. Specifically, implement controls to prevent an individual from querying BR metadata for data integrity and foreign intelligence purposes and issue formal guidance to differentiate such queries.

S3 Input: ~~(TS//SI//NF)~~ S3 has accepted responsibility for performing the functions of the Data Integrity Analysts and determined this mission will be performed within the [redacted] Based on S3 direction, it is expected that [redacted] will have an interim procedure to perform DIA functions in place within three weeks, working toward a permanent procedure to be in place within three months.

(b)(1)
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20350901

EXHIBIT C

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 applicable law.

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

This report provides specific information regarding the number and types of demands to which we responded for the second half of 2015, as well as Foreign Intelligence Surveillance Act (FISA) demands for the first half of 2015. For comparison purposes, we included data from our prior report. During this reporting period, we acquired DIRECTV, a satellite television and internet service provider with operations both domestic and international. Information for DIRECTV has been included in both the U.S. and International sections of this report. Overall, demands for DIRECTV data represent less than 1% of the total demands received by AT&T.

Privacy Advocacy

We remain committed to the privacy of AT&T's customers around the world. As such, we have been engaged in a number of initiatives during this reporting period. AT&T continues to join with other technology companies and public interest groups to advocate for limits on the government's ability to obtain customer communications stored abroad. AT&T believes that law enforcement should respect the laws of other countries and work through established treaties. Our country's respect for international data protection standards will help ensure that the privacy interests of Americans are also respected by other countries.

We are active members in a number of organizations focused on human rights and privacy. We are a member of the Telecommunications Industry Dialogue, which is a group of telecommunications operators and vendors who jointly address freedom of expression and privacy rights in the telecommunications sector in the context of the UN Guiding Principles on Business and Human Rights. We are also an active member of the Digital Due Process

Coalition. Through this Coalition we work with other companies, privacy advocates, and think tanks, to advocate for the simplification, clarification, and unification, of the legal standards in the Electronic Communications Privacy Act, while preserving the tools necessary for government agencies to enforce the laws, respond to emergencies, and protect the public.

NATIONAL SECURITY DEMANDS

National Security Letters	Jan. – June 2015	July – Dec. 2015
▪ Total Received	500 – 999	500 – 999
▪ Number of Customer Accounts	2,500 – 2,999	2,000 – 2,499
Foreign Intelligence Surveillance Act[1]	**July – Dec. 2014**	**Jan. – June 2015**
▪ Total Content	0 – 499	0 – 499
○ Customer Selectors Targeted	16,500 – 16,999	14,000 – 14,499
▪ Total Non-Content	0 – 499	0 – 499
○ Customer Selectors Targeted	0 – 499	0 – 499

TOTAL U.S. CRIMINAL & CIVIL DEMANDS

Total Demands	Jan. – June 2015	July – Dec. 2015
(Federal, State and Local; Criminal and Civil)	145,104	142,876
▪ Subpoenas	107,982	105,033
○ Criminal	96,781	91,568
○ Civil	11,201	13,465
▪ Court Orders (General)	18,574	18,768
○ Historic	14,934	15,409
○ Real-Time (Pen registers)	3,640	3,359
▪ Search Warrants / Probable Cause Court Orders		
○ Historic	12,347	13,141
▪ Stored Content	3,398	3,656
▪ Other	8,949	9,485
○ Real-Time	6,201	5,934
▪ Wiretaps	1,416	1,306
▪ Mobile Locate Demands	4,785	4,628

DEMANDS REJECTED / PARTIAL OR NO DATA PROVIDED

(Breakout detail of data included in Total U.S. Criminal & Civil Demands)

	Jan. – June 2015	July – Dec. 2015
Total	46,406	37,589
▪ Rejected/Challenged	2,525	2,467
▪ Partial or No Information	43,881	35,122

LOCATION DEMANDS

(Breakout detail of data included in Total U.S. Criminal & Civil Demands)

	Jan. – June 2015	July – Dec. 2015
Total	37,973	38,367
▪ Historic	28,745	29,444
▪ Real-Time	8,545	8,184
▪ Cell Tower	683	739

EMERGENCY REQUESTS

	Jan. – June 2015	July – Dec. 2015
Total	56,329	62,829
▪ 911	43,670	47,971
▪ Exigent	12,659	14,858

[1] The USA Freedom Act and the Department of Justice impose a six-month delay for reporting this data.

NATIONAL SECURITY DEMANDS

Our reporting on National Security Letters and court orders issued pursuant to FISA (collectively "National Security Demands") is governed by the USA Freedom Act. *See* Section 604 of the USA Freedom Act. That statute only permits us to report data in defined numeric ranges and for certain time periods.

National Security Letters are required administrative 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.

Consistent with the above guidance, our report includes the range of National Security Letters and FISA demands served on us and the "customer selectors targeted" by those respective demands.[2]

TOTAL U.S. CRIMINAL & CIVIL 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 criminal law. The existence of federal, state and local investigating authorities in the U.S. means that we can receive demands from thousands of different law enforcement entities.

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.

[2] The term "customer selectors targeted" is statutory. *See* 50 U.S.C. § 1874.

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 law 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 probable cause court order or search warrant. If the requesting agency has failed to send the correct type of demand, we reject the demand.

Types of Legal Demands

The reporting category "Total U.S. Criminal & Civil Demands" reflects 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, i.e., an attorney. They are used in both criminal and civil cases, typically to obtain testimony or written business documents such as calling records and basic subscriber information such as the name and address listed on the billing account.

- **General Court Orders** are signed by a judge. We consider "general" court orders to be 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 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. 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. In both the criminal and civil context, General Court Orders were used to obtain historic information like billing records or records relating to usage of a wireless device.

- **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 is required for all real-time precise location information (like GPS),

real-time content (such as content obtained through wiretaps), and stored content (like stored text and voice messages).

Foreign-Originated Demands for Information about a U.S. Consumer or Business

If we receive an international demand for information about a U.S. customer, whether an individual or business, we refer it to that country's Mutual Legal Assistance Treaty (MLAT) process. We did not receive any international demands for information about a U.S. customer from a country that does not have an 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.

DEMAND 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 civil and criminal legal demands we received by the type of location information (historic and real-time) requested. Demands for location information seek precise GPS coordinates of the device or call detail records that reflect the location of any cell site processing a call. We also get demands for cell tower searches, which ask us to provide all telephone numbers registered on a particular cell tower for a certain period of 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. We disclose both the total number of demands and the total number of cell tower searches. For instance, if we received one court order that included two cell towers, we count that as one demand for two searches. For the 739 cell tower demands during this period, we performed 1,993 searches. We also maintain a record of the average time period that law enforcement requests for one cell tower search, which was 2 hours and 13 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 precise location information. For the production of historic cell site location, however, the standard varies. We require a General Court Order, search warrant, or probable cause court order, depending on the applicable state and federal laws.

EMERGENCY REQUESTS

The numbers provided in this category are the total of 911-originated inquiries and exigent requests that we processed during this reporting period. 911-originated inquiries are those that help locate or identify a person in need of emergency assistance. "Exigent requests" are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies. In order to protect your privacy, we require a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we will share information sought by an exigent request.

INTERNATIONAL DEMANDS

In our last Transparency Report we discussed AT&T's expansion into Mexico through the acquisitions of Iusacell and Nextel Mexico. During this reporting period, AT&T further expanded its international operations through the acquisition of DIRECTV. DIRECTV has operations in a number of countries in Latin America where it provides satellite television service and, in some locations, broadband connectivity.

The "International Demands" category represents the number of civil and criminal legal demands originating outside the U.S. and related to AT&T's operations in foreign countries. These demands are for information about consumers who reside in other countries, businesses that operate in other countries, and URL/IP (website/Internet address) blocking requests from foreign governments.

The Diverse Services AT&T Provides Internationally Affects the Types and Volume of Demands We Receive

- **Business Services:** AT&T provides telecommunications and IT services to the foreign offices of large multi-national business customers. In all foreign countries where AT&T supports these customers, AT&T primarily receives demands for subscriber information and IP or URL blocking.

- **Consumer Mobility Services:** Mexico is the only country outside of the U.S. where AT&T provides consumer mobility service. Accordingly, AT&T received legal demands similar to those it receives in the U.S., including demands for subscriber information, location information and real time content.

- **DIRECTV:** In all Latin American countries where AT&T provides DIRECTV consumer satellite television service we primarily receive requests for subscriber information. In those Latin American countries where DIRECTV also provides broadband service, we also received demands for IP or URL blocking.

A Few Additional Points

- The IP or URL blocking requests come from countries that require us to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate. These demands 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.
- While AT&T may provide internet access in some foreign countries, we do not have the ability to control the content of any websites other than AT&T's own sites. Accordingly, while we did receive and comply with demands from foreign governments to block access to websites in their countries during this reporting period, we did not receive demands to remove content from websites (nor would we be able to do so).
- During this reporting period we did not receive any requests from any foreign governments to produce any stored content. Internationally, AT&T does not store content unless the customer directs us to do so as part of our services.
- Finally, the laws governing the international demands that we receive differ by country. We respond to these demands based on each country's laws.

INTERNATIONAL DEMANDS

Total International Demands[3]	Jan. – June 2015	July – Dec. 2015
Argentina		
• Subscriber Information	0	354
• IP Blocking	6	2
Australia		
• Subscriber Information	0	1
• IP Blocking	0	0
Belgium		
• Subscriber Information	0	0
• IP Blocking	9	5
Brazil		
• Subscriber Information	n/a	44
• IP Blocking	n/a	1
Canada		
• Subscriber Information	n/a	2
• IP Blocking	n/a	0
Chile		
• Subscriber Information	n/a	5
• IP Blocking	n/a	1
Colombia		
• Subscriber Information	0	528
• IP Blocking	4	12
Ecuador		
• Subscriber Information	n/a	28
• IP Blocking	n/a	n/a
France		
• Subscriber Information	0	2
• IP Blocking	0	0

Hungary		
• Subscriber Information	1	0
• IP Blocking	0	0
Italy		
• Subscriber Information	2	0
• IP Blocking	0	0
Peru		
• Subscriber Information	n/a	6
• IP Blocking	n/a	0
Portugal		
• Subscriber Information	0	0
• IP Blocking	3	2
Romania		
• Subscriber Information	0	0
• IP Blocking	0	4
Russia		
• Subscriber Information	0	0
• IP Blocking	180	180
Spain		
• Subscriber Information	1	1
• IP Blocking	0	0
Uruguay		
• Subscriber Information	n/a	3
• IP Blocking	n/a	n/a
Venezuela		
• Subscriber Information	n/a	702
• IP Blocking	n/a	0
Mexico		
▪ Historic: Subscriber Information / Call Detail Records	5,089	4,962
○ Location Information (Cell Site)	4,835	3,357

▪ Real-Time	379	397
○ Pen Registers / Wiretaps / Cell Site	161	139
○ Location Information (Precise)	218	258

[3] We were also required to block access to websites in India but are precluded by law from identifying the specific details about those requests.

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 D

verizon

Transparency Report 1H 2016

verizon

United States Report

The table below sets out the number of subpoenas, orders, warrants and emergency requests we received from federal, state or local law enforcement in the United States in the first half of 2016. The total number of demands (and the number of subpoenas, orders, warrants and emergency requests) in the first half of 2016 were generally comparable with the number of demands we received in prior six-month periods.

The vast majority of these various types of demands relate to our consumer customers; we receive relatively few demands regarding our enterprise customers. We do not release customer information unless authorized by law, such as a valid law enforcement demand or an appropriate request in an emergency involving the danger of death or serious physical injury.

Law Enforcement Demands for Customer Data – United States

	2013 (Full Year)	**Half of 2013***	**1st Half of 2014**	**2nd Half of 2014**	**1st Half of 2015**	**2nd Half of 2015**	**1st Half of 2016**
Subpoenas	164,184	82,092	72,342	65,816	69,524	65,663	67,433
Total Orders	70,665	35,333	37,327	33,453	37,230	33,813	33,161
General Orders	62,857	31,429	33,313	29,656	33,138	30,568	29,635
Pen Registers/ Trap & Trace Orders	6,312	3,156	3,300	3,078	3,325	2,678	2,870

verizon

Wiretap Orders	1,496	748	714	719	767	567	656
Warrants	36,696	18,348	14,977	13,050	15,081	14,248	11,798
Emergency Requests From Law Enforcement	50,000 (approx)	25,000 (approx)	24,257	26,237	27,975	25,844	23,394
Total	**321,545**	**160,773**	**148,903**	**138,656**	**149,810**	**139,568**	**135,786**

* In our first Transparency Report (published in January 2014), we reported on the full year for 2013. Since that Report, we have reported data based on half-year periods. To aid the comparison between the half-year numbers we have reported since 2013 and the full-year numbers we reported in 2013, we have simply halved the 2013 numbers in the table.

We also received National Security Letters and FISA Orders; we address them in a separate table at the bottom of this Transparency Report.

Verizon has teams that carefully review each demand we receive. We do not produce information in response to all demands we receive. We might reject a demand as legally invalid for a number of reasons, including that a different type of legal process is needed for the type of information requested. When we reject a demand as invalid, we do not produce any information.

There are a number of additional reasons why we might not produce some or all of the information sought by a demand, although we do not consider these “rejected” demands and do not calculate the number of times these occur. We often receive demands seeking information about a phone number serviced by a different provider. And, we regularly receive demands seeking data that we do not have – perhaps the data sought were of a type we have no need to collect or were older than our retention period. Moreover, if a demand is overly broad, we will not produce any information, or will seek to narrow the scope of the demand and produce only a subset of the information sought. Additionally, it is not uncommon for us to receive legal process and in response produce some information, but not other information. For instance, we may receive a subpoena that properly seeks subscriber information, but also improperly seeks other information, such as stored content, which we cannot provide in response to a subpoena; while we would provide the subscriber information (and thus would not consider this a rejected demand), we would not provide the other information. We include all demands we receive in our table above, whether we provided data in response or not.

verizon

Subpoenas

We received 67,433 subpoenas from law enforcement in the United States in the first half of 2016. We are required by law to provide the information requested in a valid subpoena. The subpoenas we receive are generally used by law enforcement to obtain subscriber information or the type of information that appears on a customer's phone bill. We continue to see that approximately half of the subpoenas we receive seek only subscriber information: that is, those subpoenas typically require us to provide the name and address of a customer assigned a given phone number or IP address. Other subpoenas also ask for certain transactional information, such as phone numbers that a customer called. The types of information we can provide in response to a subpoena are limited by law. We do not release contents of communications (such as text messages or emails) or cell site location information in response to subpoenas.

In the first half of 2016, the 67,433 subpoenas we received sought information regarding 136,180 information points, such as a telephone number, used to identify a customer. These customer identifiers are also referred to as "selectors." On average, each subpoena sought information about 2.0 selectors. The number of selectors is usually greater than the number of customer accounts: if a customer had multiple telephone numbers, for instance, it's possible that a subpoena seeking information about multiple selectors was actually seeking information about just one customer. We have also determined that during the first half of this year, just like during the prior periods, approximately 75 percent of the subpoenas we received sought information on only one selector (and thus only one customer), and over 90 percent sought information regarding three or fewer selectors (and thus three or fewer customers).

Orders

We received 33,813 court orders in the second half of 2015. These court orders must be signed by a judge, indicating that the law enforcement officer has made the requisite showing required under the law to the judge. The orders compel us to provide some type of information to the government.

General Orders. Most of the orders we received – 30,568 – were "general orders." We use the term "general order" to refer to an order other than a wiretap order, warrant, or pen register or trap and trace order. We continue to see that many of these general orders require us to release the same types of basic information that could also be released pursuant to a subpoena. We do not provide law enforcement any stored content (such as text messages or email) in response to a general order.

"Pen/Trap" Orders and Wiretap Orders. A small subset – 3,245 – of the orders we received in the first half of 2015 required us to provide access to data in real-time. A pen register order requires us to provide law enforcement with real-time access to phone numbers as they are dialed, while a trap and trace order compels us to provide law enforcement with real-time access to the phone numbers from incoming calls. We do not provide any content in response to pen register or trap and trace orders.

We received 2,678 court orders to assist with pen registers or trap and traces in the second half of last year, although generally a single order is for both a pen register and trap and trace. Far less frequently, we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. We received 567 wiretap orders in the second half of 2015.

verizon

Warrants

We received 11,798 warrants in the first half of 2016. To obtain a warrant a law enforcement officer must show a judge that there is “probable cause” to believe that the evidence sought is related to a crime. This is a higher standard than the standard for a general order. A warrant may be used to obtain stored content (such as text message content or email content), location information or more basic subscriber or transactional information.

Content and location information

Content. We are compelled to provide contents of communications to law enforcement relatively infrequently. Under the law, law enforcement may seek communications or other content that a customer may store through our services, such as text messages or email. Verizon only releases such stored content to law enforcement with a probable cause warrant; we do not produce stored content in response to a general order or subpoena. During the first half of 2016, we received 5,054 warrants for stored content.

Location information. Verizon only produces location information in response to a warrant or order; we do not produce location information in response to a subpoena. The laws in some areas of the country require law enforcement to obtain a warrant to get location information, but the laws in other areas permit law enforcement to obtain a court order. In either scenario, the demand we receive for location information is approved by a judge. In the first half of this year, we received approximately 18,935 demands for location data: as in the past, about two-thirds of those were through orders and one-third were through warrants.

In addition, we received approximately 5,993 warrants or court orders for “cell tower dumps” in the first half of this year. In such instances, the warrant or court order compelled us to identify the phone numbers of all phones that connected to a specific cell tower during a given period of time.

Emergency requests

Law enforcement requests information from Verizon that is needed to help resolve serious emergencies. We are authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency requests, in accordance with the law. To request data during these emergencies, a law enforcement officer must certify in writing that there was an emergency involving the danger of death or serious physical injury to a person that required disclosure without delay. These emergency requests are made in response to active violent crimes, bomb threats, hostage situations, kidnappings and fugitive scenarios, often presenting life-threatening situations. In addition, many emergency requests are in search and rescue settings or when law enforcement is trying to locate a missing child or elderly person.

We also receive emergency requests for information from Public Safety Answering Points (PSAPs) regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers, or PSAPs, throughout the country. PSAPs receive tens of millions of calls from 9-1-1 callers each year, and certain information about the calls (name and address

verizon

for wireline callers; phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Yet a small percentage of the time PSAP officials need to contact the telecom provider to get information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller.

In the first half of 2016, we received 23,394 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury. We also received 16,721 emergency requests from PSAPs related to particular 9-1-1 calls from the public for emergency services during that same period.

National Security Demands

The table below sets forth the number of national security demands we received in the applicable period. Under section 603 of the USA Freedom Act we are now able to report the number of demands in bands of 500. Previously reported figures are still reported in bands of 1000. We note that while we are able to provide some information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited.

	Jan. 1, 2013 – June 30, 2013	**July 1, 2013 – Dec. 31, 2013**	**Jan. 1, 2014 – June 30, 2014**	**July 1, 2014 – Dec. 31, 2014**	**Jan. 1, 2015 – June 30, 2015**	**July 1, 2015 – Dec. 31, 2015**	**Jan. 1, 2016 – June 30, 2016**
National Security Letters	0-999	0-999	0-999	0-999	0-999	0-499	0-499
Number of customer selectors	2000-2999	2000-2999	2000-2999	2000-2999	2000-2999	500-999	500-999
FISA Orders (Content)	0-999	0-999	0-999	0-999	0-499	0-499	*

verizon

Number of customer selectors	4000-4999	3000-3999	3000-3999	2000-2999	1500-1999	1000-1499	*
FISA Orders (Non-Content)	0-999	0-999	0-999	0-999	0-499	0-499	*
Number of customer selectors	0-999	0-999	0-999	0-999	0-499	0-499	*
** The government has imposed a six month delay for reporting this data*							

National Security Letters

In the first half of 2016, we received between 0 and 499 NSLs from the FBI. Those NSLs sought information regarding between 500 and 999 “selectors” used to identify a Verizon customer. (The government uses the term “customer selector” to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of “customer accounts.” An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.)

The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.

verizon

FISA Orders

The government requires that we delay the report of any orders issued under the Foreign Intelligence Surveillance Act for six months. Thus, at this time, the most recent FISA information we may report is for the second half of 2015.

Content

From July 1, 2015 through December 31, 2015, we received between 0 and 499 FISA orders for content. Those orders targeted between 1,000 and 1,499 “customer selectors” used to identify a Verizon customer.

Non-Content

From July 1, 2015 through December 31, 2015, we received between 0 and 499 reportable FISA orders for non-content. Some FISA orders that seek content also seek non-content; we counted those as FISA orders for content and to avoid double counting have not also counted them as FISA orders for non-content. Those orders targeted between 0 and 499 “customer selectors.”

EXHIBIT E

(TS//SI//NF) Mobility Business Records Flow Significantly Increases Volume of Records Delivered Under BR FISA
By [redacted] on 2011-08-30 1440

(TS//SI//NF) On 29 August, FAIRVIEW started delivering Mobility Business Records traffic into MAINWAY under the existing Business Record (BR) FISA authorization. The intent of the Business Records FISA program is to detect previously unknown terrorist threats in the United States through the cell chaining of metadata. This new metadata flow is associated with a cell phone provider and will generate an estimated 1.1 billion cellular records a day in addition to the 700M records delivered currently under the BR FISA. After extensive dialogue with the consumers of the BR data, repeated testing, a push to get this flow operational prior to the tenth anniversary of 9/11, and extensive coordination with external entitites via our OGC (to include: FBI, DOJ, ODNI, and FISC) NSA received approval to initiate this dataflow on August 29, 2011. Analysts have already reported seeing BR Cellular records in the Counter Terrorism call-chaining database queries.

POCs: [redacted] S3531, [redacted] & [redacted] S35324, [redacted]

EXHIBIT F

ABOUT THE AUTHOR

George Molczan is Director of Network Services for General Communication, Inc. (GCI) in Anchorage, Alaska. In addition to his responsibilities for the operation and maintenance of GCI's switched network, he is responsible for compliance with court orders, subpoenas, and search warrants from attorneys and law enforcement agencies and frequently testifies regarding telephony issues.

George's career includes a broad range of technical and managerial experience with Pacific Northwest Bell (now part of Qwest) as well as GCI. His diverse background makes him comfortable discussing corporate budgets or explaining call routing, installing trap and trace devices, and discussing telephony-related legislation. He can be reached by e-mail at george@gmolczan.com.

A LEGAL AND LAW ENFORCEMENT GUIDE TO TELEPHONY

Addressing Technical, Legal and Police Issues Relating to the Interface and Interaction with Communication Service Providers

By

GEORGE MOLCZAN

Director, Network Services–Operations
General Communications, Inc.
Anchorage, Alaska

CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704

ISBN 0-398-07574-3
ISBN 0-398-07575-1

Library of Congress Catalog Card Number: 2004062067

With THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

Printed in the United States of America
CR-R-3

Library of Congress Cataloging-in-Publication Data

Molczan, George.
A legal and law enforcement guide to telephony : addressing technical, legal and police issues relating to the interface and interaction with communication service providers / by George Molczan.
p. cm.
Includes index.
ISBN 0-398-07574-3 -- ISBN 0-398-07575-1 (pbk.)
1. Telephone companies--United States. 2. Telephone--United States. 3. Telephone companies--Corrupt practices--United States. 4. Telephone--Law and legislation--United States. 5. Law enforcement--United States. 6. Electronic surveillance--United States. I. Title.

HE8815.M65 2005
384.3'02'43632--dc22

2004062067

PREFACE

A *Legal and Law Enforcement Guide to Telephony* addresses technical and legal issues relating to attorney and law enforcement's interface and interaction with communication service providers. The goal is to provide legal and law enforcement practitioners with factual, informative, and easy-to-understand information about telephone company interworkings, their networks, and operation. The range of subjects includes local, long distance, and cellular services; private phone systems (PBX and KTS); 911 systems; telephone fraud; pay phones; customer premises wiring; and new technologies including voice over the Internet (VoIP).

Telephone calls, like people, leave fingerprints known as *call records* for virtually every call that passes through the telephone network. These fingerprints are useful to law enforcement, aiding in reconstructing events and tracking the movement of individuals. Although competition in the local, long distance, and cellular industries has increased the need to generate a greater volume of call records, the typical subpoena does not result in an exhaustive discovery. Many telephone company personnel are unaware that some of these records exist, where they are, or how to find them. Unlike investigations where trained law enforcement specialists look for and gather evidence, law enforcement agencies are dependent on telephone company personnel to look for and gather call records. Armed with the knowledge presented here, investigators will be prepared to probe the innerworkings of telephone companies guiding the search for evidence.

It is not the intent of the author, the publisher, or the sellers of this text to provide legal guidance nor do they claim to be qualified to do so. While this text discusses various technical aspects of monitoring the telephone network or a subscriber's telephone line, the author,

publishers and sellers make no representation of the legality of these practices. The reader is advised to seek legal counsel in regard to any and all monitoring of any portion of the telephone network or requesting or application of information received from a communication service provider.

CONTENTS

Page

Preface v
List of Tables xi

Chapter

1. THE TELCO AND THE LAW 3
   Law Enforcement and Telephone Service Providers 3
   Telephone Company and Customer Rights 12

2. FRAUD AND NUISANCE CALLS 15
   Fraud by Service Providers 15
   Fraud Committed by Nonservice Providers 18
   Nuisance and Harassment Calls 25
   Denial-of-Service Attacks 28

3. CALL RECORDS: FINGERPRINTS IN THE NETWORK 31
   Call Records (Electronic Fingerprints) 31
   Tracking a Call Through the Telephone Network 37

4. THE SWITCHED TELEPHONE NETWORK 41
   Elements of a Telephone Network 41
   Call Types 52
   Trunking and Switching Hierarchy 55
   A Detailed Look at a Central Office 59
   Digital Subscriber Line (DSL) 63
   Wireline to Wireless Interconnection and Call Flow 67
   Caller ID 68
5. VOICE OVER THE INTERNET 71

Voice Over the Internet, Quality of Service, and Architectures . . . 71
VoIP Calling-Line Features . . . 80
Number Portability with VoIP Services . . . 80
911 Emergency Calls . . . 81
VoIP as a Way to Bypass the Local and Long-Distance Carriers . . . 82

6. COMPETITION IN THE LOCAL TELEPHONE INDUSTRY . . . 87
Forms of Competition . . . 87
The Physical Connection . . . 92

7. CELLULAR, PCS, AND SATELLITE TELEPHONE SERVICES . . . 97
Cellular Telephony . . . 97
Satellite Telephony (Low Earth Orbit) . . . 100

8. ANATOMY OF A TELEPHONE NUMBER . . . 103
The North American Numbering Plan . . . 103
The 500 Area Code–"Follow Me" Services . . . 108
Toll-Free Calling (800, 866, 877, and 888) . . . 108
Pay-Per-Call and Information Services . . . 109
Local Number Portability . . . 111
Calling Cards . . . 112
Carrier-Specific Services . . . 114

9. CUSTOMER PREMISES EQUIPMENT . . . 115
Private Branch Exchanges (PBX) . . . 115
Key Telephone Systems (KTS) . . . 130
PBX and Key System Trunking . . . 132
Answering Services . . . 134
Centrex . . . 135
Packetized CPE Systems . . . 137

10. INSIDE WIRE, CABLE, AND JACKS . . . 139
Residential Inside Wire and Jacks . . . 139
Commercial Building Wire and Cable . . . 145
Network Interface Devices . . . 146

11. EMERGENCY 911 CALL PROCESSING . . . 147
Basic 911 Systems (B911) . . . 147
Enhanced 911 Systems (E911) . . . 148
E911 for Wireless Services . . . 150
Managing 911 Telephone Number and Location Data . . . 154
Call Records for 911 Calls . . . 156

12. PAY PHONES . . . 159
Dumb Pay Phones . . . 159
Smart Pay Phones . . . 160
Inside Wire for Pay Phones . . . 164
Pay Phone Fraud . . . 164

Index . . . 165

Chapter 3

CALL RECORDS: FINGERPRINTS IN THE NETWORK

Whether you call them call records, call detail records (CDR), station message detail records (SMDR), or automatic message accounting (AMA) records, they are the electronic fingerprints left by calls using the telephone network. Throughout this book, examples are presented of where call records (fingerprints) can be found. This chapter endeavors to pull this information together and examine call records in detail. The term *call record* is used in this book to refer to all of the call types listed, unless specifically stated.

3.1 CALL RECORDS (ELECTRONIC FINGERPRINTS)

Law enforcement agencies (LEA) should remember when writing a subpoena or court order for a service provider to make sure they understand what they are asking for and that they are talking the same language as the service provider. An example is where a LEA served a subpoena on a local telephone company asking for call records associated with a telephone number. They were expecting either paper or electronic records in a form similar to those in Figure 3.1 for originating and terminating calls. What they received were paper copies of the originating calls as seen on a subscriber invoice. When the LEA asked the local service provider about the difference they were told, "You get what you ask for." The service provider went on to say, "If you want all the other information you need to ask for AMA records."

Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
400	50500	6	288	10/21/02	17:21:44	2065550112	5095550192	3956		3784
400	50500	6		10/21/02	17:22:14	4085550174	2065550164	88	2276	

Figure 3.1. Sample call records.

3.1.1 Call Records and Who Keeps Them.

Virtually all communication service providers keep call records for a variety of reasons. Table 3.1 lists the most common reasons.

Table 3.1
REASONS COMMUNICATION CARRIERS KEEP CALL RECORDS

- Billing for long-distance calling (Interexchange Carriers)
- Calls to 800 numbers (long-distance companies supporting dial-around compensation for pay phone providers)
- Calls to 900 numbers (long-distance service providers for billing pay-per-call charges)
- Billing for local calls on a time or usage basis (metered/measured billing)
- Feature usage (billed on a per-use basis)
  - Last call return
  - Last number redial
  - Customer-initiated call trace
- Carrier traffic–carrier's carrier (one carrier billing another for transporting their traffic)
- Originating and terminating access billing (local and long-distance service providers)
- Airtime and access billing (cellular, PCS, and satellite phone carriers)
- Pay phone providers (paying commissions to premises owners and claiming dial-around compensation)
- Calling card companies (paying carriers to transport traffic)
- Client billing (PBX systems and Centrex installations)
- Calls to 911 call centers (for tracking purposes)
- Telecom network and traffic engineers

Following are some examples of various call types and information about which service providers have call records and why. It is quickly apparent that there are electronic fingerprints in a lot of places. Like real fingerprints, knowing where to look is the key. In these examples pay attention to the words wireline and wireless as they can easily be misread.

Wireline-to-Wireline Local Call, Same Service Provider

Figure 3.2 depicts the simplest of call types, which is between two wireline (also known as landline) subscribers sharing the same service

provider switch. In this example there is no reason for the local service provider to generate, collect, and store call records. If subscriber A is a PBX extension, the PBX operator may have a call record with call details.

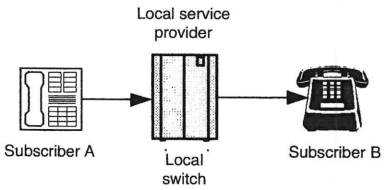


Figure 3.2. Wireline-to-wireline local calls–sharing the same switch.

To ensure call records are available, an LEA should request a *trap* on the line. If the local service provider offers usage sensitive billing they may already have call records for all outgoing calls.

Wireline-to-Wireline Local Call, Different Service Provider

A wireline-to-wireline call between local service providers as shown in Figure 3.3 has a greater chance of generating a call record without a trap on the line. In this case call records provide the data for the two local service providers to bill each other for local access. In other words, they charge each other for terminating local calls from their competitors' subscribers. Again, if the originating station is a PBX extension, the PBX operator may have call record information.

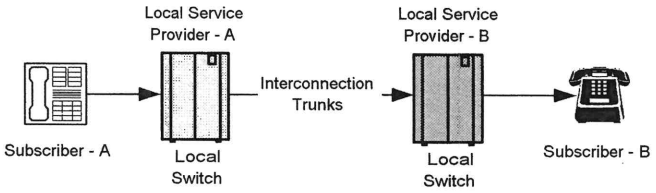


Figure 3.3. Wireline-to-wireline local calls–between different service providers.

Wireline-to-Wireless Local Call

In Figure 3.4 a call is shown between a wireline subscriber and a wireless subscriber. In this scenario both carriers will have call records

with details of the call. Both carriers use the call record information for billing local access charges. The wireless carrier will use the call record information for billing airtime to the wireless subscriber.

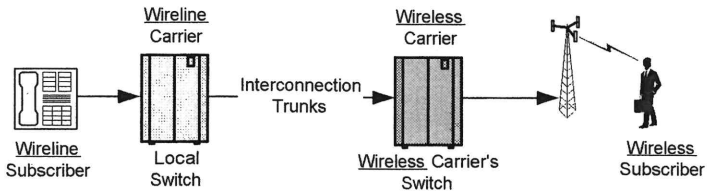


Figure 3.4. Wireline-to-wireless call.

Wireline long-distance call

The long-distance call shown in Figure 3.5 depicts two different calls. The first call originates from the wireline subscriber A, routing through the long-distance carrier switch (IXC) and terminating to wireline subscriber B. For this call wireline carrier 1 would have call records for billing of the long-distance call to subscriber A. The long-distance carrier will have call records for billing transport of the call to the originating wireline carrier (wireline carrier 1). The terminating local carrier (wireline carrier 2) will have call records used for billing terminating access to the long-distance carrier.

If the long-distance call that originated with wireline subscriber A had terminated to a wireless subscriber, the originating local carrier and the long-distance carriers will have the same call records as if the call terminated with a wireline subscriber. The wireless carrier will have call records for billing terminating access to the long-distance carrier and for billing the wireless subscriber for airtime.

Calls to, From, and Between Wireless Subscribers

The preceding section described a call terminating to a wireless subscriber and which carriers would have call records for that call. Calls from and between wireless subscribers follow the same format. If the call is long distance and the wireless carriers are using an interexchange carrier (IXC) to transport the call, the IXC will have call records with information about the call.

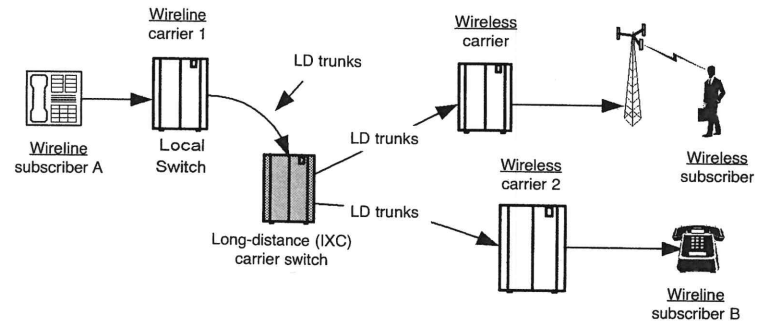


Figure 3.5. Wireline originated long-distance call.

3.1.2 Elements of a Call Detail Record

In this book call records are referred to in the manner used by LEAs. The information required for LEA use is a subset of the total information available in a call record. Most LEA requests for call records are to determine call originating and terminating numbers (calling and called ANI), date, and duration. Table 3.2 lists elements in a call record from a class 5 central office switching system. The elements shown in italics are those normally of interest to LEAs and are what telephone companies supply.

Table 3.2
ELEMENTS OF A CALL RECORD

- Switch ID (carrier dependent)
- Structure code
- Call type (defines the type of call record, local, long-distance)
- CIC (carrier identification code, for long distance)
- *Date call originated* (MMDDYY)
- *Time call originated* (in 24-hour format)
- *The originating telephone number* (10-digit format)
- *Terminating telephone number* (10-digit format, even if it is a local call where the originating party only dials 7 digits)
- *Elapsed time*[1] (Measured from when calling party went off hook and usually measured in 1/100 second)
- *Originating trunk group*
- Originating trunk group member number
- Originating trunk seizure time

1. In some cases the time will be two fields, the answer time and the disconnected time.

- Originating trunk disconnect time
- *Terminating trunk group*
- Terminating trunk group member number
- Terminating trunk seizure time
- Terminating trunk disconnect time

Figure 3.6 is representative of call records after service providers sort and collect the records in response to a request from an LEA.

Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
400	50500	6	288	10/21/02	17:21:44	2065550112	5095550192	3956		3784
400	50500	6		10/21/02	17:22:14	4085550174	2065550164	88	2276	

Figure 3.6. Call records as presented to a law enforcement agency.

In the first data record shown in Figure 3.6, the originating trunk group field is blank indicating the originating telephone number is a working number on the switch that generated the call record and it is served by the line side of the switch. If the call originated from a PBX or key telephone system (KTS) being served by a trunk group, that trunk group number would appear in the originating trunk group field. In the second data record the opposite is true. The second record, not having a terminating trunk group, indicates the switch that serves the called number generated the call record. In all of these examples the time is shown in seconds.[2]

3.1.3 Overlapping Call Records

There are two reasons why call records can overlap in time. The first is the terminating subscriber has the line feature call waiting. For example the two call records in the dotted line box in Figure 3.7 are for a subscriber that has call waiting. Note that the second call record starts and ends within the duration of the preceding call record. Simply put, while the subscriber was on the first call they received a second call, answered that call, talked for 22 seconds, hung up, and returned to the first call.

2. When converting seconds to hours, minutes, and seconds, you cannot simply divide by 60 or 360 unless it comes out without a remainder. For example, 1,332 seconds divided by 60 gives a result of 22.2. This is 22 2/10 minutes or 22 minutes and 12 seconds. The common error is to think of this as 22 minutes and 2 seconds.

Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
400	50500	6	288	10/21/02	17:21:44	2065550112	5095550192	3956		3784
400	42130	6		10/21/02	17:22:14	4085550174	2065550116	88	2276	
400	62120	6		10/21/02	18:20:22	2065550112	5095550192	440		
400	42130	6	077	10/21/02	18:21:23	4085550174	5095550192	22	2276	
400	62120	6		10/21/02	20:14:11	5095550192	5095550116	282		
400	50500	6	077	10/21/02	20:14:42	5095550192	4075550132	110		3428

Figure 3.7. Overlapping call records.

Another example of overlapping call records is where a subscriber has three-way calling, call add-on, or conference calling. The last two call records in Figure 3.7 depict this scenario. Again, the second record starts and ends within the duration of the preceding record for the same originating number. In this example, the line that originated the first call, 31 seconds later originated a second call (call add-on or three-way calling), which accounts for the second call record of the pair.

3.2 TRACKING A CALL THROUGH THE TELEPHONE NETWORK

Individual call records typically provide all the information necessary for an LEA to determine a call's origination. However, if the originating number is not available, multiple call records can be linked to provide a path back to the originating point. This section describes how to link call records starting with the terminating point and working backward.

3.2.1 How Call Records Record the Path of a Call

In Figure 3.8 a long-distance call is shown, as it would route through the telephone network. The call originates with subscriber A (originating telephone number 206-555-0112), routes through the IXC (long-distance) switch 3, terminating to subscriber B (terminating tele-

phone number 509-555-0192). In this scenario, three call records are generated as shown in Figure 3.9. In this example the three records are shown together, but in reality they may come from the three service providers involved in the call. Also note that this example shows all three calls originating at exactly the same time. In theory they would be close to the same start time; however, the time-of-day clocks in the individual systems are not synchronized with each other or a common time-of-day clock.[3]

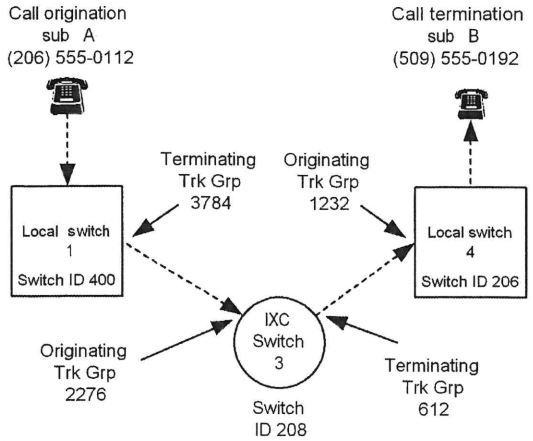


Figure 3.8. Tracking a call through the telephone network.

When analyzing call records, the originating and terminating trunk groups reference the center of the switch, which generates the call records. For example, in the second call in Figure 3.9 the originating trunk group is the trunk group where the call came into the switch whereas the terminating trunk group is the group on which the call left the switch.

3.2.2 Call Records without an Originating Telephone Number

Many requests for call records are based on the terminating telephone number, the object being to determine who called the target number. The examples in this text depict an ideal world where all call records have originating and terminating telephone numbers.

3. When matching call records, the time zone in which the call record was created needs to b considered.

Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
400	50500	6	288	10/21/02	17:21:44	2065550112	5095550192	3956		3784
Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
208	42130	6		10/21/02	17:21:44	2065550112	5095550192	3956	2276	612
Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
206	62120	6		10/21/02	17:21:44	2065550112	5095550192	3956	1232	

Figure 3.9. Multiple call records for a typical long-distance call.

However, real-world experience produces call records without the originating telephone numbers, as shown in Figure 3.10. Although this example has all zeros for the originating number, it could be all ones or blank.

Switch ID	Structure Code	Call Type	CIC	Date	Time	Orig Number	Term Number	Elapsed Time	Orig. Trunk Group	Term Trunk Group
206	50500	6	288	10/21/02	17:21:44	0000000000	5095550192	38	1232	

Figure 3.10. Call records without an originating telephone number.

With the information provided in the call record shown in Figure 3. 10 the following conclusions can be drawn:

1. The terminating number is served directly by the switch that produced the call record. This is based on the fact that there is no terminating trunk group. With this information it is possible to start putting together how the call routed. Figure 3.11 is the first phase of the route.

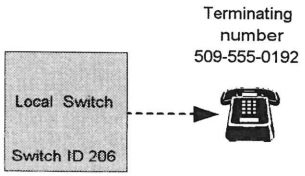


Figure 3.11. Putting together call record information to chart a call route.

2. The second known fact is the call originated from another switch or a PBX, as there is an originating trunk group. Adding this information gives us the route shown in Figure 3.12.

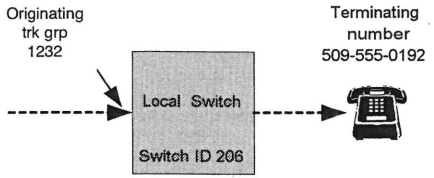


Figure 3.12. Continuing the create a drawing of a call route.

At this point a request would have to be sent to the local service provider who supplied the call record, (Figure 3.10) requesting the identification of their originating trunk group 1232. It could be one of the following:

- Another switching system of the same local exchange carrier (LEC) as the terminating switch
- A competitive LEC (which could be a mobile service operator or cell phone company)
- A long-distance or interexchange carrier (IXC)

In any case, it is now up to the LEA to contact the connecting carrier and request the call record that matches the one they have. It will be necessary to provide the connecting carrier with the terminating telephone number, date, and time, and the terminating carrier. (Note: The time of day may not match exactly; however, the elapsed time should be within a couple seconds.)

Although this is a tedious, time-consuming method of tracing a call back to its origination, it does work.

Chapter 4

THE SWITCHED TELEPHONE NETWORK

Many law enforcement and legal personnel are familiar with the telephone network, or at least they are familiar with how it used to be. Local telephone service as described in this chapter is based on a noncompetitive environment, meaning there is a single local exchange carrier (LEC) that serves a geographic area. Prior to competition in the local exchange telephone business, operation of the telephone network was straightforward. That is, it was straightforward compared to what happens in the industry with competition. Chapter 6 covers many of the same network elements described in this chapter, but it deals with competition in the local telephone business and the complexities competition brings. The telephone network described in this chapter is the public switched telephone network (PSTN) also referred to as the landline or wireline network. Chapter 7 will deal with cellular, PCS, and satellite telephone services.

The fundamentals of the PSTN, as covered in this chapter, provide law enforcement and legal professionals with a foundation for understanding the advanced concepts covered later in this book.

4.1 ELEMENTS OF A TELEPHONE NETWORK

As an introduction to telephony this section reviews the physical aspects of a switched telephone network. The following section covers the fundamentals of call processing and the physical properties of telephone lines (copper and wireless), along with a look inside a telephone company central office.

EXHIBIT G

DYNAMIC PAGE -- HIGHEST
POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO
USA AUS CAN GBR NZL

(S//SI) FAIRVIEW and STORMBREW: 'Live' - On the Net

FROM: [redacted] and [redacted]
Special Source Operations (S332)
Run Date: 11/19/2003

(TS//SI) Two special source collection programs - S332's FAIRVIEW and STORMBREW - are producing SIGINT successes by "living on the global intelligent network." In September of this year, FAIRVIEW quietly turned on a new DNI (Digital Network Intelligence) collection capability that quickly proved a valuable source of intelligence: A&P's Office of Proliferation and Arms Control (S2G21) issued the first SIGINT product report sourced from this new access on September 24. Then, less than a month later, the first E-series product report (extremely sensitive serialized reports sent to a limited audience) was issued by International Security Issues, (S2C21). Many other offices now use this collection, as well - the FAIRVIEW DNI access is extremely high-volume and delivers a very broad target set covering all SIGINT product lines. For example, the initial deployment of the FAIRVIEW DNI access, for e-mail only, is now forwarding more than one million emails a day to the keyword selection system at NSAW.

(TS//SI) STORMBREW has a complementary large-scale DNI collection effort (covername PERFECTSTORM) that is just about ready for prime time. As the large-scale effort was being developed, STORMBREW deployed several QRC (Quick Reaction Capability) collection systems that have yielded critical intelligence supporting the Global War on Terrorism. STORMBREW engineers then worked with FAIRVIEW engineers to transfer this collection architecture to FAIRVIEW. Recently, FAIRVIEW identified the "other side" of one of the STORMBREW QRC links, and was able to use the same collection architecture to rapidly put this new link on cover. This type of complementary access provides the A&P analysts with more complete coverage of their target. In addition, STORMBREW and FAIRVIEW personnel worked side-by-side with CES personnel to add Voice over IP processing capabilities to both of these accesses to further exploit the targets' communications.

(TS//SI) In addition to email, FAIRVIEW and STORMBREW are also collecting metadata, or data about the network and the communications it carries. For September 2003 alone, FAIRVIEW captured several trillion metadata records - of which more than 400 billion were selected for downstream processing or storage. This metadata will be used to enable the surgical collection of much smaller amounts of target-rich data - which should extend beyond FAIRVIEW and STORMBREW to many other DNI accesses across NSA. This metadata is flowing to MAINWAY (contact chaining

database) today, and a major interface to the Knowledge System Prototype (KSP) is only days away from its operational debut. Both the STORMBREW and FAIRVIEW teams are working closely with the Network Analysis Center, the Collection Strategies and Requirements Center, and analysts throughout A&P to foster metadata exploitation, focus the access, improve the selectors and filters, and hunt for targets within the access. This collaborative process is the foundation for SIGINT success on the Net.

(TS//SI) FAIRVIEW and STORMBREW also provide other major international accesses that support all A&P SIGINT product lines. In a recent complementary modernization effort, the FAIRVIEW and STORMBREW programs quadrupled SIGINT production from these circuit-switched accesses, only a few months after implementation. As the FAIRVIEW and STORMBREW programs continue to expand their "live" presence on the global net, we are expecting even greater insight into the net itself, and the communications of our targets, resulting in similar SIGINT production gains from these packet-switched accesses.

Comments/Suggestions about this article?

Information Own [redacted] S012[redacted]
Page Publisher: [redacted], S0121, [redacted]
Last Modified: 11/09/2012 / Last Reviewed: 11/09/2012

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007
DECLASSIFY ON: 20320108

EXHIBIT H

TOP SECRET//COMINT//NOFORN

Dataflow Diagrams

April 2012

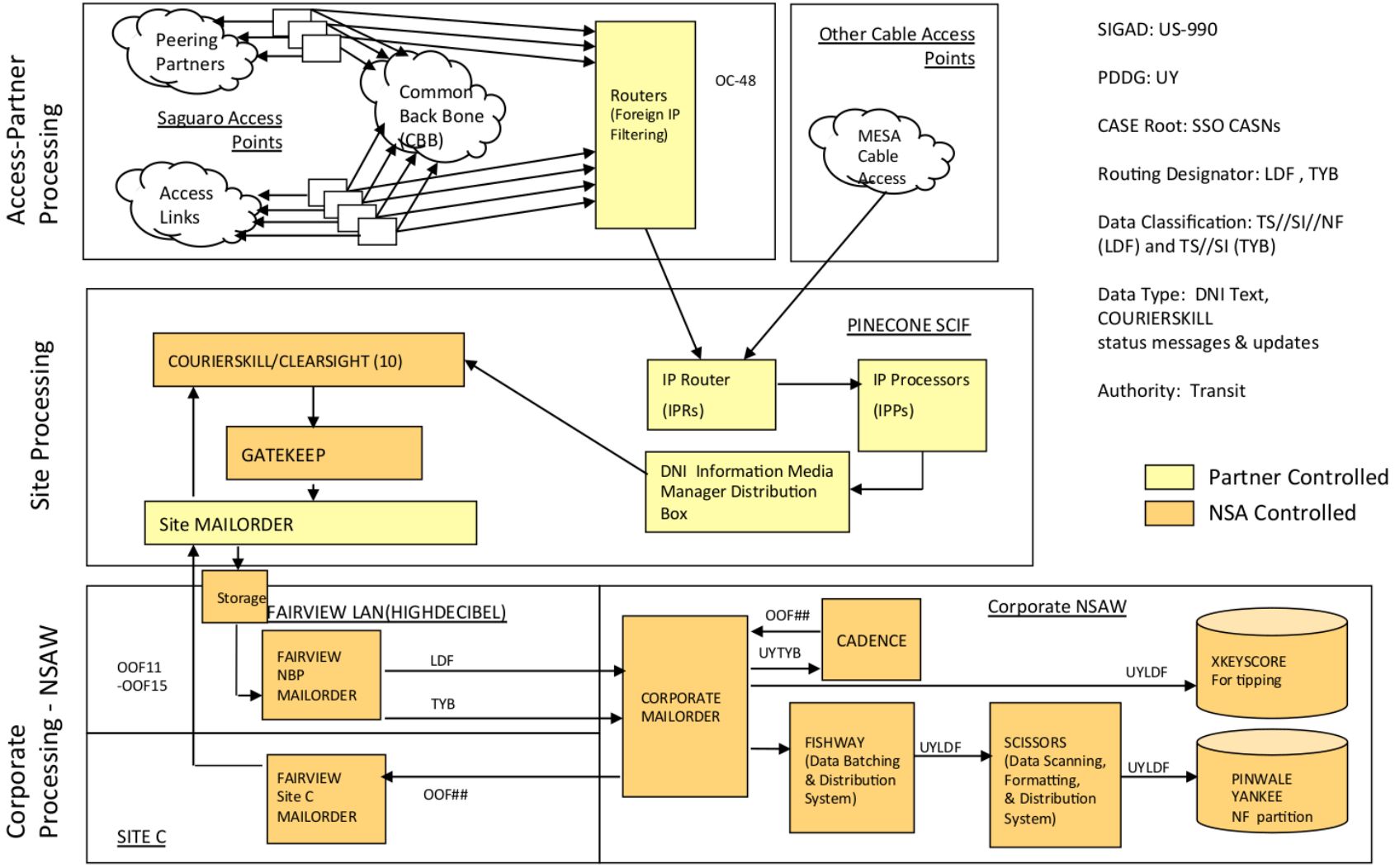
Note: Please refer to previous diagrams for decommissioned systems.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20361101

TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN

Transit DNI Content (BUGCATCHER)



SIGAD: US-990

PDDG: UY

CASE Root: SSO CASNs

Routing Designator: LDF , TYB

Data Classification: TS//SI//NF (LDF) and TS//SI (TYB)

Data Type: DNI Text, COURIERSKILL status messages & updates

Authority: Transit

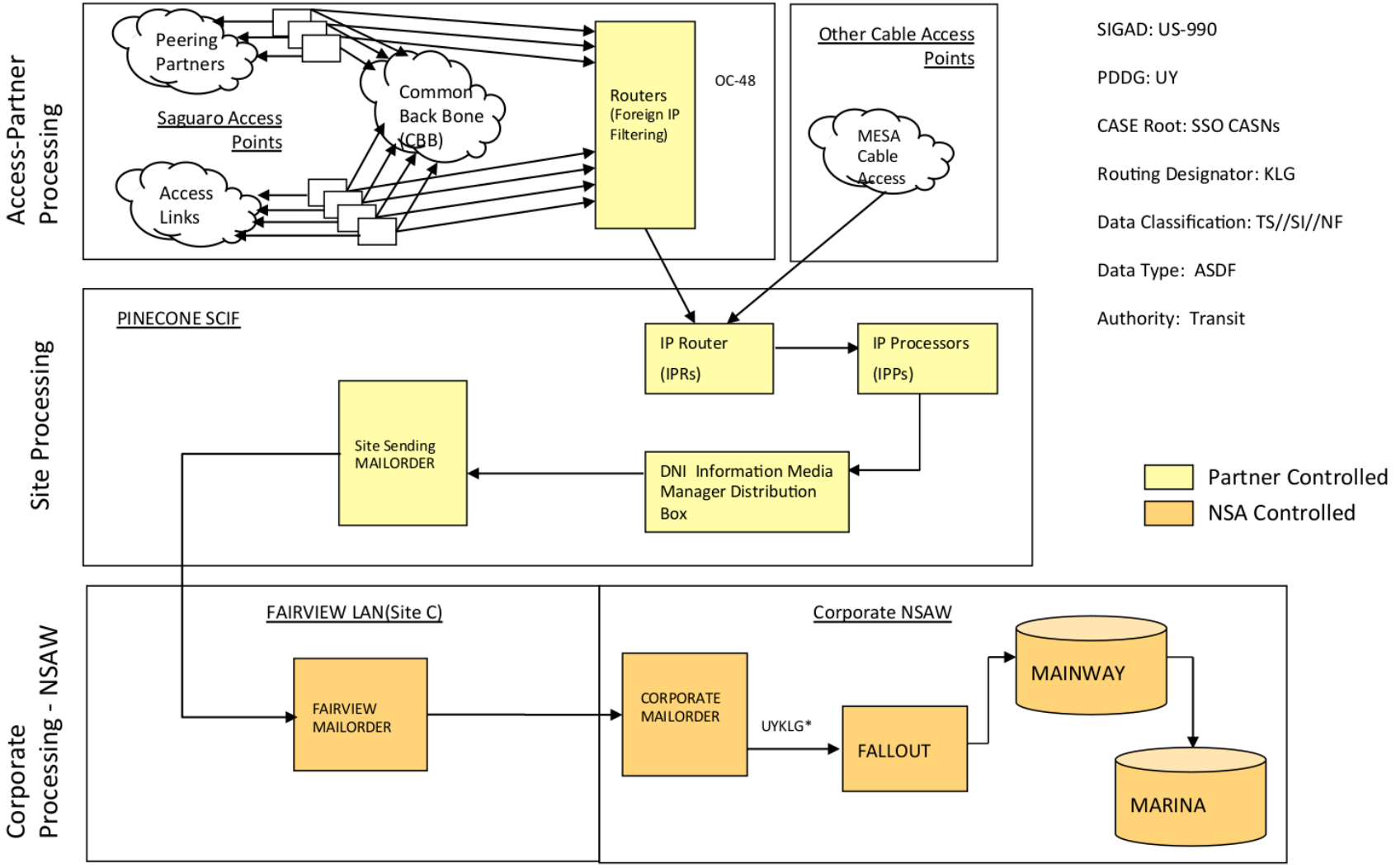
Partner Controlled

NSA Controlled

TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN

Transit DNI Metadata (IMDRs)



SIGAD: US-990

PDDG: UY

CASE Root: SSO CASNs

Routing Designator: KLG

Data Classification: TS//SI//NF

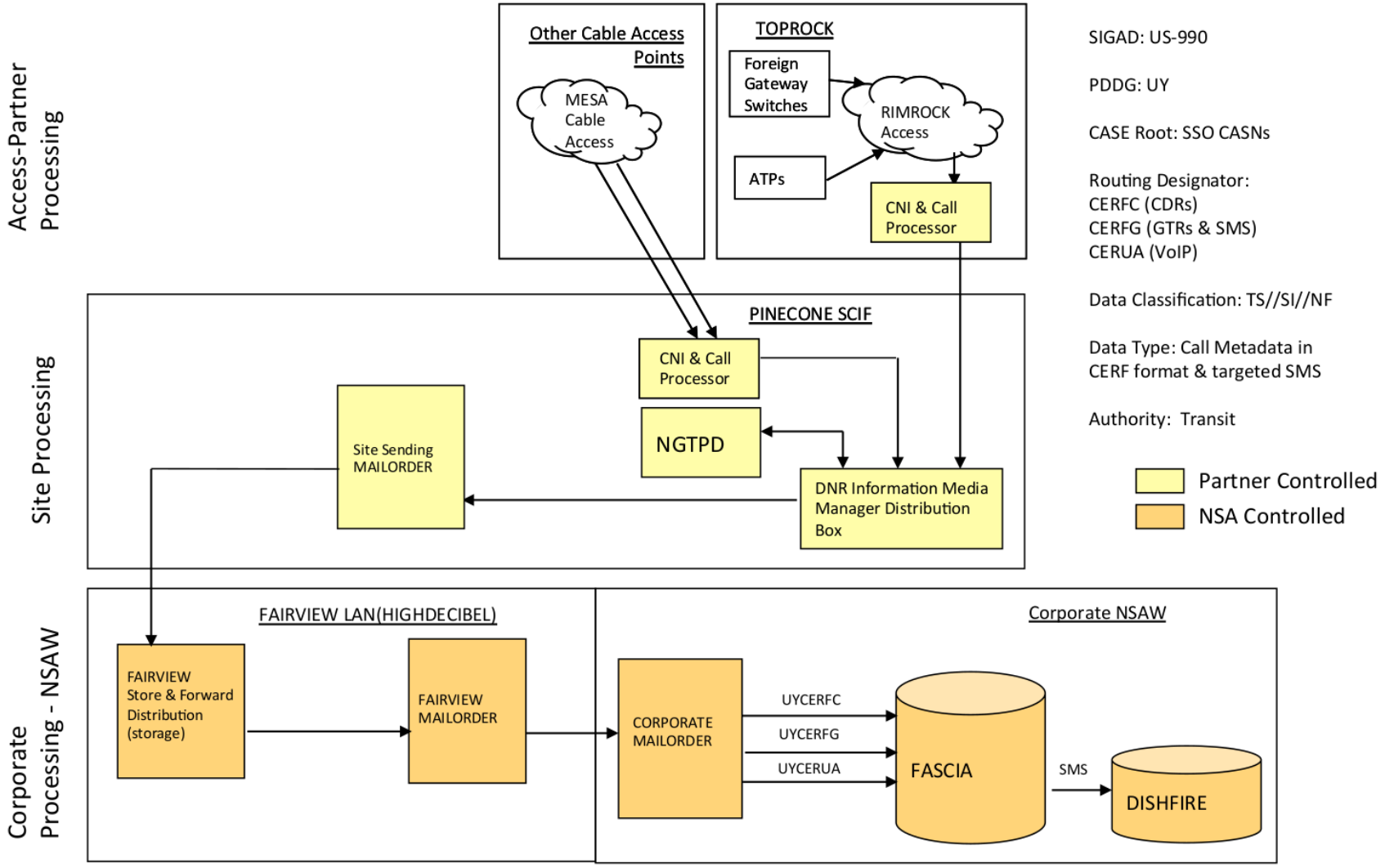
Data Type: ASDF

Authority: Transit

TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN

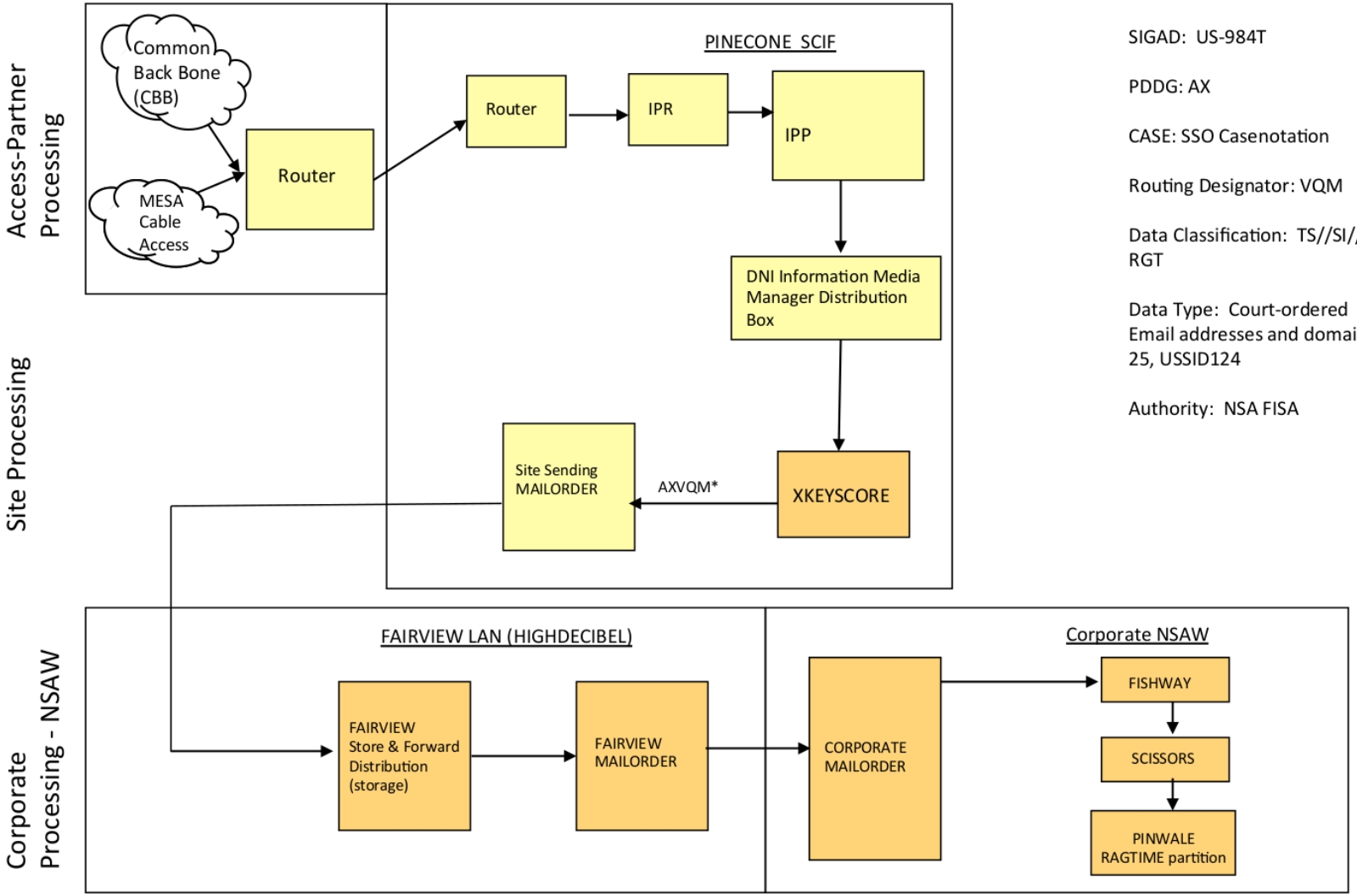
Transit DNR Metadata & SMS



TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN

FAIRVIEW NSA FISA Email



SIGAD: US-984T

PDDG: AX

CASE: SSO Casenotation

Routing Designator: VQM

Data Classification: TS//SI//NF//RGT

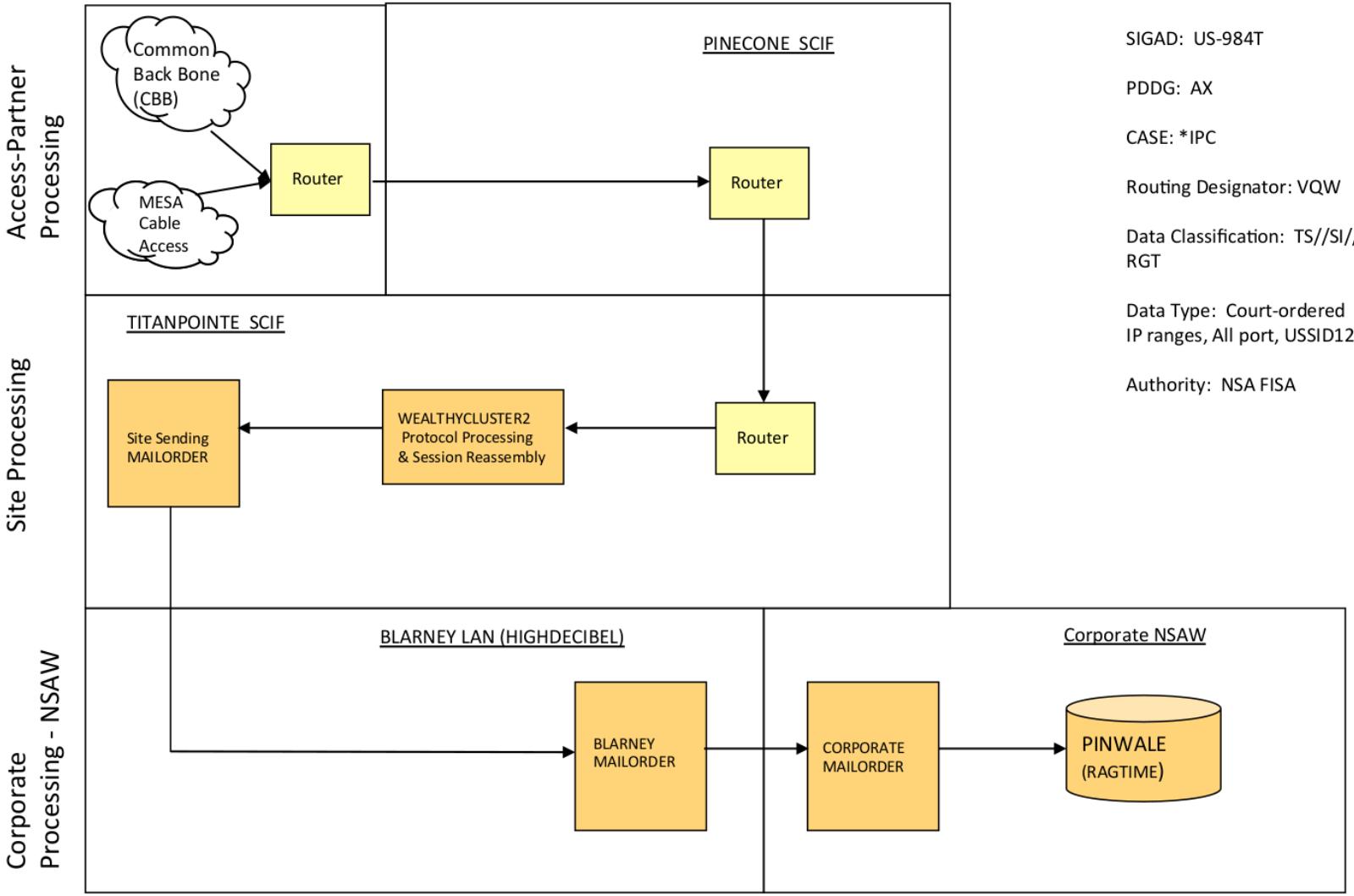
Data Type: Court-ordered Email addresses and domains, Port 25, USSID124

Authority: NSA FISA

TOP SECRET//COMINT//NOFORN

TOP SECRET//COMINT//NOFORN

FAIRVIEW NSA FISA IP



SIGAD: US-984T

PDDG: AX

CASE: *IPC

Routing Designator: VQW

Data Classification: TS//SI//NF//RGT

Data Type: Court-ordered IP ranges, All port, USSID124

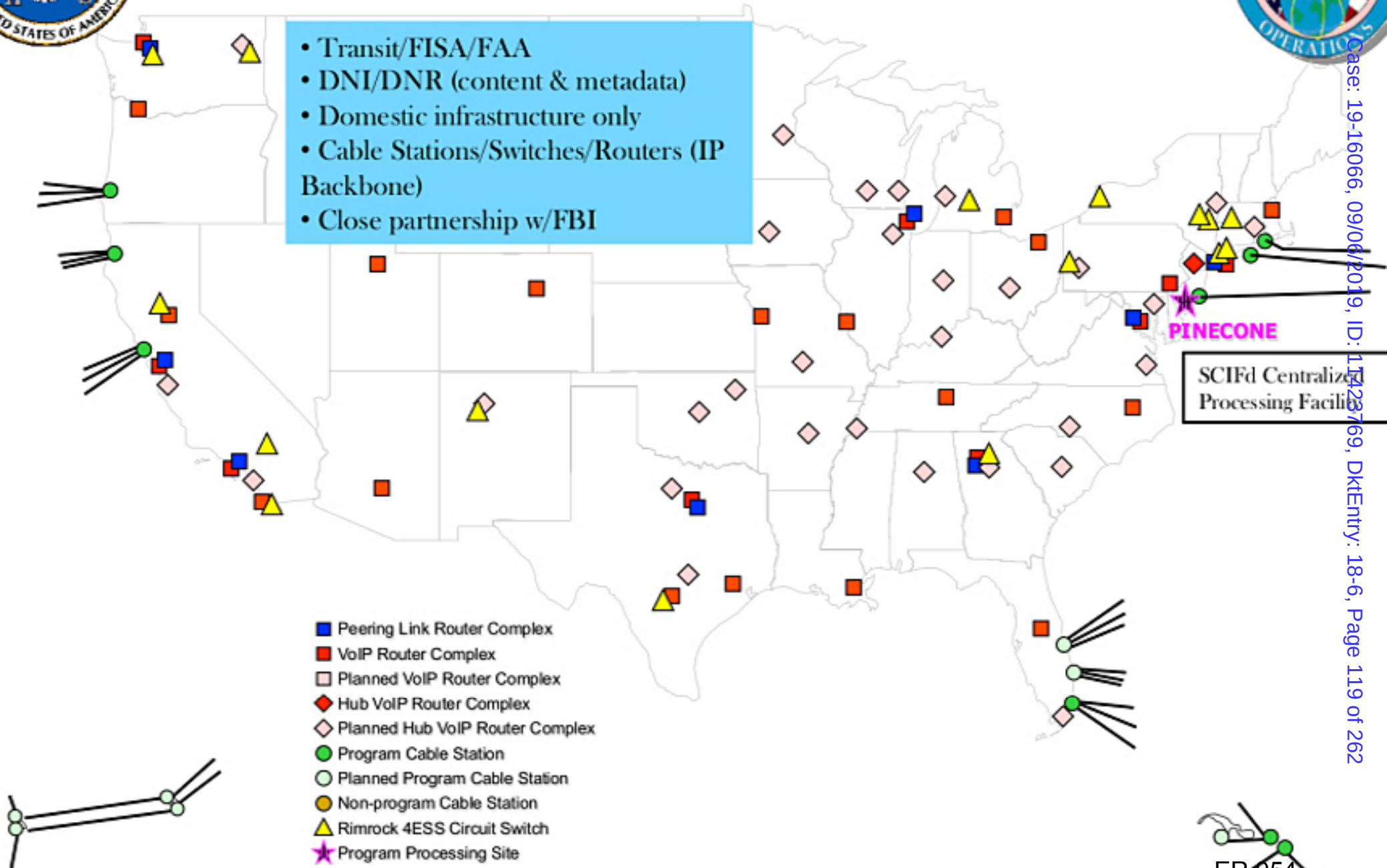
Authority: NSA FISA

TOP SECRET//COMINT//NOFORN

EXHIBIT I

FAIRVIEW At a Glance

- Transit/FISA/FAA
- DNI/DNR (content & metadata)
- Domestic infrastructure only
- Cable Stations/Switches/Routers (IP Backbone)
- Close partnership w/FBI



CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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 **Declaration of Phillip Long** The Honorable Jeffrey S. White

I, PHILIP LONG, declare as follows:

1. I have personal knowledge of the facts set forth below and if called as a witness could and would competently testify thereto.

2. I worked for AT&T and its successor and related entities from 1972 to 1988 and from 1996 to 2015.

3. I am a graduate of the University of Nevada, Las Vegas in business management. I have an FCC 1st class radio license with a telegraph and radar endorsement.

4. In 1972 I began working for AT&T's subsidiary Nevada Bell in Las Vegas, Nevada. My position was Long Lines transmission man. I worked on microwave transmission. At that time, microwave transmission was a principal means of long distance communication.

5. In 1977, I transferred to San Francisco, California and began working for Pacific Bell, another AT&T subsidiary. I was stationed at 555 Pine Street but some of my work was done at AT&T's 611 Folsom Street location in San Francisco. My position was chief transmission man.

6. I left Pacific Bell in 1988 to work for Alameda County. My duties involved radio and microwave communications, installation, and repair.

7. I returned in 1996 to work for Pacific Bell. My position was senior systems technician. All of my work involved setting up, connecting, and maintaining Internet circuits, including connecting customers to AT&T's Internet backbone circuits. I was stationed in Concord, California at a Network Data Plant Service Center, a central location for managing data transmissions services. My work included responsibility for the 611 Folsom Street facility. I did work both onsite and remotely at 611 Folsom Street. Much of the work in setting up, testing, and routing circuits is now done remotely from service centers, where technicians can perform the work electronically.

8. My work location transferred to San Ramon, California Network Operations Center in approximately 2000. But Pacific Bell kept significant equipment in Concord, including frame relay (and later ATM) equipment that connects customers directly to the Internet backbone. These connections did not run through any facilities in San Francisco.

9. The Concord frame relay connection to the Internet backbone encompassed

customers in a large region of California, including at various times locations such as Oakland, Fresno, Visalia, Bakersfield, Castaic.

10. Other Pacific Bell locations in Northern California had similar frame relay equipment that allowed for direct connections to the Internet backbone, including San Jose and Sacramento.

11. Sometime in the first half of the 2000s, we began receiving service orders that made no sense to me from an engineering or business standpoint.

12. We were directed to start rerouting Internet backbone connections through 611 Folsom Street, rather than through the nearest frame relay or ATM switch.

13. Among the rerouted connections that that I recall were the Internet backbone connections for Concord, San Jose, Sacramento, Oakland, Walnut Creek, Castaic, Bakersfield, Fresno, Visalia, Ukiah, and Reno, Nevada.

14. Internet backbone connections between these locations were also rerouted. For example, what had been a direct Internet backbone link between Sacramento and Los Angeles now became a link from Sacramento to 611 Folsom Street, followed by a link from 611 Folsom Street to Los Angeles. Likewise, what had been a direct Internet backbone link from Concord to Sacramento became an indirect link running from Concord to 611 Folsom Street to Sacramento.

15. Rerouting Internet traffic in this circuitous and indirect manner made no sense from an engineering or business standpoint.

16. Another example is Concord. Rather than joining the Internet backbone directly in Concord, Internet traffic arriving in Concord was first sent to 611 Folsom Street and then sent back from 611 Folsom Street to Concord, where it then connected to the Internet backbone. This round-trip was a pointless waste of circuit capacity.

17. Similarly, Internet traffic that had once connected to the Internet backbone in San Jose was now sent to 611 Folsom Street instead to connect to the Internet backbone there.

18. In addition, San Francisco-bound traffic that was once sent to 555 Pine Street was now sent to 611 Folsom Street instead, even though 555 Pine Street was a larger hub with more communications connections.

19. The effect was to centralize Internet traffic at 611 Folsom Street that previously had connected to the Internet backbone at numerous, more decentralized locations. Internet traffic was no longer being routed to the closest or most efficient point of connection to the Internet backbone.

20. I recall that we also rerouted circuits from San Diego and Los Angeles in Southern California to 611 Folsom Street to connect to the Internet backbone there. Because there are numerous Internet backbone connection points in Southern California, bringing that traffic to San Francisco to connect to the Internet backbone made no sense.

21. In my work at 611 Folsom Street in the 2000s, I became familiar with Room 641A on the sixth floor. Room 614A was always kept locked and ordinary technicians were not allowed inside. This was contrary to standard practice in every other similar facility I have ever worked in. Technicians need access to everyplace that cable runs in a facility in order to do their work.

22. I was instructed to bring fiber optic cable connected to equipment in 611 Folsom Street and leave the terminating end of the cable on the floor in front of the door to Room 641A. This is contrary to standard practice, which is to terminate fiber optic cable into a known piece of equipment. Later, we connected a fiber optic terminal jack to the end of the cable outside of Room 641A. Another fiber optic cable then ran from the fiber optic terminal jack into Room 641A.

23. In 2009, the Network Operations Center transferred to Sacramento, but it remained responsible for circuits and operations in 611 Folsom Street as well as elsewhere in Northern and Central California.

24. I continued working at the Sacramento Network Operations Center until my retirement in 2015.

//

//

//

//

//

//

//

25. During my time at the Sacramento Network Operations Center from 2009 to 2015, the Internet circuits I have described above continued to be routed to 611 Folsom Street and to connect to the Internet backbone there.

I declare under penalty of perjury under the laws of the United States the foregoing is true and correct and if called as a witness I could and would so testify.

Executed on September 21, 2018.

Philip Long

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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 **Declaration of Dr. Brian Reid** The Honorable Jeffrey S. White

I, Brian Reid, declare as follows:

1. I have been asked by plaintiffs' counsel to apply my expertise and experience in network operation and engineering to examine and analyze the evidence described herein. In this declaration, I describe my background, outline my conclusions, and explain the basis and the reasoning that support those conclusions. If called as a witness, I could and would testify to the matters stated herein.

2. Based on my expertise, after carefully reviewing all of the documents in this case, I believe it is very likely that the plaintiffs' communications passed through the peering site at AT&T's Facility at 611 Folsom Street at least once during the 17 years at issue in this case, and that these communications—along with the rest of the traffic passing over all of the peering-link fibers into which splitters were installed at AT&T's 611 Folsom Street Facility—were replicated, with one replica copy redirected by the optical splitter assemblies described by Mark Klein and the other sent to its original destination. Based on the documents reviewed, and my expertise in network engineering, it is virtually impossible for me to imagine a scenario in which this did not happen.

BACKGROUND

3. I am a telecommunications and data-networking expert with over 40 years of experience studying, developing, operating, and improving communications systems. I have extensive knowledge of and experience with international telecommunications infrastructure and the technology regularly used for lawful surveillance pursuant to warrants and court orders. I have been involved in the development of several critical Internet technologies, including email, web, and document representation and transmission.

4. I am currently the Director of Operations at Internet Systems Consortium (ISC), an organization that develops and distributes internet software and uses that software to operate critical infrastructure. We meet payroll by offering support contracts for the use of our free software. ISC also participates in the development of standards for the internet and is a significant contributor to the Internet Engineering Task Force.

5. I have worked at ISC for over 13 years. In my current role as Director of Operations, which I have held for almost three years, I have management and lead technical responsibility for ISC's server and network operations, staff IT, and for one of the 13 clusters of DNS root servers that serve the entire internet, worldwide. I was previously a Senior Member of Technical Staff in the Office of the Chief Technical Officer (CTO), where I was the sole employee in the office and essentially carried out the duties of CTO: I took part in every technical and business decision made at ISC and reported directly to the company president. When it was needed, I served as the Director of Corporate Communications (I am an experienced writer and editor), and as the Director of Operations and Engineering.

6. I received a Bachelor of Science in Physics from the University of Maryland in 1970. While obtaining my undergraduate degree, I worked for the University of Maryland Computer Science Department as a Systems Programmer, where I developed operating system software and compiler for the Univac 1100 series of computer, funded by NASA. I also produced the software for one of the ALSEP research modules on Apollo 17 (the Lunar Surface Gravimeter).

7. After graduating from the University of Maryland, I worked in the airline industry on scheduling software for four years before joining Carnegie Mellon University as a research scientist in 1974. In 1975, I entered graduate school at Carnegie Mellon, and was awarded a PhD in Computer Science in 1980. My dissertation research developed the Scribe word processing system, for which I received the Association for Computing Machinery's Grace Murray Hopper Award in 1982. Most scholars consider Scribe to be the inspiration for HTML, which is the *lingua franca* of the World Wide Web.

8. From 1980 to 1987, I was an assistant professor of electrical engineering at Stanford University. In 1984, I was a recipient of the National Science Foundation's Presidential Young Investigator Award. While at Stanford, I conducted research regarding the university's connection to the Internet, and developed system architecture for VSLI (very-large-scale integration) systems, including the SUN workstation [Stanford University Network], which was a modular personal computer system designed for use in an Ethernet-type local network. While I was at Stanford, malicious actors first began showing up on the internet, and I was involved in or took

the lead in every attempt by Stanford and its law enforcement partners to locate the evildoers and stop them.

9. In 1987, I joined Digital Equipment Corporation (DEC), as a Consulting Engineer at the Western Research Laboratory (WRL). While working at WRL, I worked with Paul Vixie to develop one of the first connections between a corporate network and the Internet, known as "Gatekeeper." The protection techniques we developed evolved into what is now called a network "firewall." I taught classes in internet technology to large numbers of DEC employees, and helped the corporation build its internal internet. Former New York Times reporter John Markoff told me that when the FBI arrested computer hacker Kevin Mitnick in 1995, he was carrying false identification saying that he was me. (The book *Takedown* describes this arrest).

10. In 1995, after working in WRL for eight years, I was promoted to Director of my own DEC research group, the Network Systems Laboratory (NSL). Under my leadership, NSL developed the first independent Internet exchange point as the Internet became available for commercial use in the 1990s. An independent exchange point is one that is not owned or controlled by any of its users, in much the same fashion that an airport is not owned or controlled by any of the airlines that use it. My laboratory also led the company-wide project to build one of the first Web search engines. My Network Systems Laboratory was responsible for making our search engine fully accessible to the entire internet.

11. In 1999, I joined Bell Labs Research Silicon Valley (BLRSV), a startup venture of Lucent Technologies, as Laboratory Director. Under my leadership, BLRSV developed affordable fiber to the home (FTTH) technology, which provided unprecedented high-speed internet access via the installation and use of optical fiber from a central point directly to individual buildings such as residences, apartment buildings, and businesses.

12. When Lucent collapsed in 2001, I joined Carnegie Mellon University as a Professor of the Practice of Computer Systems at the University's nascent Silicon Valley branch, located at the NASA Ames Research Center at Moffett Federal Airfield in Mountain View, California. During my time as a professor at Carnegie Mellon Silicon Valley, I conducted research and infrastructure management and worked with NASA on networking technology for the International

Space Station and on developing a multi-disciplinary, multi-institutional High-Dependability Computing Program (HDCP) to improve NASA's capability to create and operate dependable software.

13. In 2002, I joined Google as the Director of Operations. The primary focus of my job responsibilities had to do with Google's networking capabilities.

14. In 2004, I left Google to become a self-employed consultant.

15. In 2005, I joined my current employer, ISC, as the Director of Operations and Engineering.

16. The conclusions that I draw below are based on on my professional training and experience, in addition to the following information, as explained in more detail below: the Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Section 702 Report"); the AT&T documents attached to the Declaration of Mark Klein; the facts and events personally observed by Mr. Klein, as set forth in his declaration (but not the conclusions he draws from those facts and events described); the facts and events personally observed by James Russell, as set forth in his declaration (but not the conclusions he draws from those facts and events described).

17. One of the AT&T documents (Ex. C to the Klein Declaration, "Study Group 3 LGX/Splitter Wiring, San Francisco /Issue 1, 12/10/02," at p. C-3) lists a number of devices. The Russell declaration states that these devices are present at AT&T's 611 Folsom Street Facility. I am familiar with and have first-hand knowledge of nearly all of the listed devices. (I have no first-hand knowledge of Narus systems but have read the documentation that was available at the time).

18. I am not receiving any compensation for my work as an expert in this matter.

SUMMARY OF CONCLUSIONS

19. My conclusions can be summarized as follows:

20. First, the technological setup at 611 Folsom Street, San Francisco, as described in the AT&T documents and in Mr. Klein's declaration, copies and redirects all communications passing over all of the peering-link fibers into which the splitters were installed.

21. Second, it is very likely that plaintiffs' communications passed through a peering link at AT&T's 611 Folsom Street Facility at least once during the 17 years at issue in this case. Communications pass through peering links when they travel from one network to another, *e.g.*, from AT&T to Verizon or Sprint. But the precise route that communications take as they travel from network to network vary; internet routing is not static. Because of the volatile nature of internet routing, and because many email communications are routed over temporary routes chosen by a router, it is unfathomable to me that in 17 years, at least one of plaintiffs' communications did not travel via the peering links described in the AT&T documents at the 611 Folsom Street Facility, a major Internet peering point. The same is true for a peering link at any other major peering point.

22. Third, it is likely that plaintiffs' communications—along with the rest of the traffic passing over all of the peering-link fibers into which splitters were installed at AT&T's 611 Folsom Street Facility—have been copied and redirected by optical splitter assemblies described by Mr. Klein in his declaration. This is because:

a. What Mr. Klein describes is a technological setup that *passively* copies all traffic passing over all of the peering-link fibers into which the splitters were installed. The optical splitting device described by Mr. Klein does not and cannot study the contents of a transmission to make a decision about whether to copy it. The splitter copies everything. The brand of splitter noted in Mr. Klein's declaration does not even use electricity. It is purely optical.

b. It would not make sense to use an active device such as a router or switch to do inline searching of every communication routed through it because of cost and performance issues. The number of such devices needed would be in the hundreds or even thousands, and they would slow down all traffic.

c. Monitoring the "to" and "from" addressing information in an email, along with the subject line and email body, requires first capturing and reassembling most of the body of the email. This means that, in order to search for "selectors," the NSA architecture must capture and reconstitute an entire transaction (message or group of messages) before analyzing any of it. As explained below, the PCLOB Section 702 Report confirms that the NSA captures the entire

contents of an email message, even if they intend to look only at its "to," "from," or "subject line" information.

23. Fourth, conducting surveillance at the peering connections between AT&T's "Internet backbone" and non-AT&T Internet providers is consistent with surveillance aimed at "one-end foreign" communications.

EXPLANATION OF THE BASIS FOR MY CONCLUSIONS

Certain Network Infrastructure Is Required To Send Information And Communications Over The Internet.

24. Internet transmission systems are extremely complex. There are many thousands of pages of documentation on how it all works, hundreds of textbooks to assist learning, and often a new technology requires revising an existing specification. This section is therefore just a brief outline of how information travels over the internet. Explanations of network operation usually reference the "ISO 7-layer model," whose formal name is "ISO/IEC 7498-1," which is a conceptual model for thinking about, characterizing and standardizing the different functions necessary for a telecommunication or computing system, without regard to its underlying structure. Wikipedia notes ISO/IEC 7498-1 "is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols."[1] The specification of the ISO 7-layer model predates the development of the internet. The ISO 7-layer model is thus described as a good way to talk about networks but no longer a suitable way of building them. Despite there not being an exact match between the vocabulary of the ISO 7-layer model and the architecture of the internet today, because the different functions necessary for a computing system remain the same.

25. When an email message is sent, it moves first from the sender's computer to a mail server. That mail server locates the recipient's mail server and initiates a transmission of the email's data stream to the recipient. Messages, such as emails, must be formulated into a layer-4

[1] Wikipedia, "OSI model," https://en.wikipedia.org/wiki/OSI_model (last updated Sep. 6, 2018).

stream (pursuant to the Transmission Control Protocol, or TCP). As part of the delivery process, this layer-4 stream is divided into individual packets, each transmitted separately. When the packets are presented to the next layer, the routing layer (layer 3), the routing devices (routers) choose the "next hop" of the transmission path based on their routing tables (which are used to determine where data packets traveling over a network will be directed). That hop delivers the packet to another router, which uses its own routing tables to continue to move the packet closer to its destination. At the time a packet is transmitted via these routers, there is no central control and no global specification of the path to be taken. Misconfigured routers can cause packets to be routed in circles, never to reach their destination.

26. The most important concept for this declaration is that, on the internet, routers (networking devices) determine the path taken by a packet—not circuits. This is an important distinction between the Internet and phone networks. Circuits are discrete (specific) paths between two or more points along which signals can be carried over the internet. Although there are actual circuits (usually fiber optic circuits) involved in the Internet, and although data is ultimately transmitted over those circuits, these circuits do not have any involvement in determining the path taken by a packet. This is a job performed only by routers, and they can decide to send different packets along different routes/circuits. Because routers are aware only of their connections to the "next hop" and not of any global end-to-end path, it is theoretically possible (though unlikely) for each packet in a transmission to take a different path to their mutual destination.

27. Next, the routing device presents the packets to the next layer, the network layer (layer 2). If a layer-3 device (*e.g.*, a router or server) presents to a layer-2 network (*e.g.*, a fiber link or an ethernet) a packet that is too large for it, the layer-2 device is expected to divide that overlarge packet into fragments (each of which meets its size limitation) and transmit each fragment separately. The ultimate recipient must reassemble fragments into packets before the packets can be reassembled into a data stream. Different fragments can be routed over different paths across the internet.

28. There are two fundamentally different approaches to network reliability. Neither has a formal name but they are often described in classrooms and conference halls as "fortification or

agility" or "strength vs flexibility." You can build a network so that each component is as strong and reliable as you know how to make it, or you can build a network whose components are adequately strong and adequately reliable but count on nimbleness in the software to re-route data away from broken devices and damaged connections. Internet engineers usually refer to this re-routing phenomenon by saying "the internet routes around damage." In combat situations it is very difficult to destroy an internet-technology communication system by destroying its components, because surviving components will find a path that does not traverse the damaged component.

29. It is very difficult to track the path taken by a particular packet. There are test procedures ("traceroutes") that will send probe packets and report the path they took, but traceroute says nothing about the path taken by a previous packet, or that will be taken by the next packet.

30. The sender of an email can neither specify nor determine the hop-by-hop routing path taken by the packets comprising that data stream initiated when they send their message. In the vocabulary of the internet, the creation of this routing path is called "making a TCP connection to the recipient." A TCP connection has very little in common with, say, a telephone connection, because the creation of a TCP "connection" does not involve reserving resources along the transmission path or even establishing a transmission path. If the transmission path were fixed at the time that the sending began, reliability would suffer because it would not be possible for the intermediate routers to make changes to that path to bypass failure or link saturation. (It does cause the recipient *mail server* to reserve resources for the inbound stream data, which makes it accept data faster).

31. The bottom layer (layer 1), is the physical layer. This layer is responsible for sending bits across circuits. The term "internet backbone" has been used colloquially, including by the media, the PCLOB, and courts (including the Court and parties in this case), to refer to the long-haul circuits (usually fiber optic circuits) of individual large-scale ISPs like AT&T. The term harkens back to the early days of the internet, in the 1980s, when a single network, the National Science Foundation Network (NSFNET), linked together supercomputing centers at research and academic institutions across the country. In 1994, the Clinton Administration decommissioned NSFNET and privatized the network, handing the job of carrying long-distance internet traffic over

to various commercial firms. For the convenience of the Court, I use "internet backbone" in that colloquial sense for purposes of this declaration.

32. Because optical fibers are small and relatively fragile, they are encased in multiple layers of strong protective material. Because the installation of fiber optic cable is very labor-intensive, the installers usually buy cables with dozens or hundreds of individual fiber strands. It is a huge amount of work to lay a fiber optic cable on the ocean floor, so installers want that cable to have as many strands as circumstances permit. It is common to see land-based fiber optic cables with 768 strands. Undersea cables necessarily have many fewer strands (one recent high-performance transpacific cable has 6 strands); this is because the undersea cables must have signal-boosting amplifiers at intervals along the ocean floor, and those amplifiers require electric power. The electric power must be piped in from one of the ends of the cable. This imposes practical limitation. Because 6 strands used directly are not enough to meet huge and growing transmission requirements if each fiber were to carry only a single transmission channel, fiber operators multiplex numerous transmissions in one strand using different colors of light (a process called Wave Division Multiplexing, or WDM).

33. Wave Division Multiplexing of unrelated transmission channels puts a big burden on a would-be wiretapper. If you want to tap a fiber-optic cable to look for certain kinds of traffic, you must not only access the optical signal, you must demultiplex it into its component wave-divided channels. Like most electronic technology, WDM devices are improving, but at the beginning of the time frame we are discussing, 12-channel WDM multiplexors on long fiber strands were common. The owner of the fiber can send 12 times as much data over it, but the would-be wiretapper must demultiplex the channels to extract those of interest. If all 12 WDM channels are of interest, it normally takes 12 monitoring devices to watch them all. As we have noted previously, packets and fragments that are part of the same email stream transmission can be routed over different paths using different fibers and/or different wavelengths of that fiber. Putting a tap at the point where an undersea cable reaches land is certainly possible, but it is much more complex than putting a tap in some place where the ISP has already done the work of demultiplexing.

34. Unless all parties to a communication are customers of the same ISP, then at some point a transmission must be handed from the sender's ISP to the recipient's ISP. ISP's have historically been suspicious and untrusting of one another, and creating a link between two of them required difficult negotiations. No ISP wanted to put equipment on a competitor's premises. Locations that did not belong to any ISP, used only for the purpose of interconnection, were originally called NAPs (Network Access Points). If two ISPs connected at a NAP and each saw the other as being approximately its peer in size and capacity, then they would sign a "peering agreement" whereby neither would charge for the handoff. If one ISP was much larger than the other, then the larger ISP would usually refuse to "peer," instead requiring that the smaller ISP become its customer instead of its peer. Within 5 years after this type of agreement became common, the vocabulary had evolved. All of it was called "peering," and the vendor/customer relationship was called "paid peering." People stopped calling these facilities NAPs and started calling them "peering points." Peering points are the buildings where "peering links" are located. Today, even the term "paid peering" is unusual. It is all called "peering"; sometimes money changes hands and sometimes it does not.

35. The Privacy and Civil Liberties Oversight Board (PCLOB) Report's phrase "the flow of communications between communication service providers" is a description of peering links.[2]

36. If both the sender and recipient of an email message use large ISPs, then a single connection between those two ISPs might be sufficient to deliver the message. The sender's ISP routes the message to the closest facility where it peers with the recipient's ISP, and hands it off to them at that peering point. But if either or both of the parties to a communication use smaller ISPs, or overseas ISPs, then the path between them is complicated enough to require multiple handoffs at multiple peering points. I have seen situations in which 9 ISPs and 8 peering-point handoffs are involved in the transmission of one email message. Since AT&T is a large ISP, it is not unusual for email messages to transit its network even when neither the sender nor the recipient is an AT&T

[2] PCLOB Section 702 Report, at 35.

customer. AT&T provides internet service to a large number of other companies, many of which connect at peering points.

The Technological Setup Of AT&T's 611 Folsom Street Facility Copies And Redirects All Communications Passing Over All Of The Peering-Link Fibers Into Which The Splitters Were Installed.

37. The AT&T documents establish (Ex. B to the Klein Declaration, "SIMS Spitter Cut-In and Test Procedure OSWF Training, Issue 2," at p. B-20) that AT&T's 611 Folsom Street Facility served as a "Service Node Routing Complex" (SNRC) (AT&T's phrase for a "peering point," a facility in which peering connections are made) where AT&T's telecommunications network "peered" with the following internet networks: ConXio, Verio, XO, Genuity, Qwest, Allegiance, Abovenet, Global Crossings, C&W, UUNET, Level 3, Sprint, Telia, and PSINet. AT&T's 611 Folsom Street Facility also peered with circuits to two Internet Exchange Points, MAE-West (Metropolitan Area Exchange, West) and PAIX (Palo Alto Internet eXchange).

38. According to Mr. Klein's declaration, he personally observed a "splitter cabinet" during his work as a technician at AT&T at the 611 Folsom Street Facility, because he and one other technician were required to connect new fiber optic circuits to the "splitter cabinet." He also testified that starting in February 2013, the "splitter cabinet" split the light signals that contained the communications in transit to and from the internet networks listed in the previous paragraph

39. In the course of preparing this declaration, I independently analyzed the AT&T documents and the statements made by Mr. Klein in his declaration. I do not rely on Mr. Klein's description of them. For purposes of this analysis I accept as true the statements made in his declaration describing how the splitters operated, what peering points they were connected to, and that they created a complete copy of the light signals crossing those peering points, as these are all facts within his personal knowledge and observation. I do not rely on any further conclusions Mr. Klein drew from those facts he observed; instead, I analyze those facts independently. AT&T Director of Asset Protection Russell testified that the documents attached to Mr. Klein's declaration are authentic AT&T documents, and I accept this testimony as true.

40. While I was an employee Lucent, as the Laboratory Director of Bell Labs Research Silicon Valley, while exploring Lucent's optical products, I discovered the splitter devices described in the Mr. Klein's declaration in a catalog and then went to see one in person at Lucent's headquarters in New Jersey. I read all of Lucent's documentation on the splitter devices at that time and am familiar with the technology.

41. A "splitter" is a communication device that accepts one input and produces multiple outputs, each being a replica of the input. They are almost universal in cable TV installations: the inbound TV cable is connected to a splitter, each of whose outputs being connected to some device that uses the cable TV signal. An optical splitter has the same function: it accepts one inbound beam of light and produces two or more outbound beams of light. The splitters described by Mr. Klein are ADC 50/50 units (referred to in the ADC catalog as 1x2 splitters), accept one inbound optical fiber connection and deliver two outbound optical fiber connections, each of which has a (slightly diminished) copy of the input. If the transmission being monitored is carried over a wire, then an electrical splitter must be used. If the transmission being monitored is carried over a fiber optic cable strand, then an optical splitter must be used.

42. The machinery at AT&T's 611 Folsom Street Facility descried in the AT&T documents and in Mr. Klein's declaration collected all communications passing over all of the peering-link fibers into which the splitters were installed, and any other new circuits on which he installed splitters.

43. The AT&T documents describe a secret, private "backbone" network separate from the public network where normal AT&T customer traffic is carried transmitted.

44. The AT&T documents also explain that the fiber optic cables were cut, and that fiber optic splitters were installed at the cut point.

45. The AT&T documents describe a system with massive, real-time surveillance capabilities. For example, it includes a NARUS 6400, a computer that can:

- Simultaneously analyze huge amounts of information based on rules provided by the machine operator.

- Analyze the content of messages and other information, not just headers or routing information.
- Conduct the analysis in "real time," rather than after a delay.
- Correlate information from multiple sources, multiple formats, over many protocols and through different periods of time in that analysis.

46. Mr. Klein testified that the second cable was routed into a room at the facility whose access was restricted to AT&T employees having clearances from the National Security Agency (NSA). The documents indicate that similar facilities were at the time being installed in Seattle, San Jose, Los Angeles, and San Diego. The documents also reference a somewhat similar facility in Atlanta.

47. This infrastructure is capable of monitoring all traffic passing through the fiber optic cables connected to the splitters at the peering point (some of it not even from AT&T customers), including voice-over-IP (VoIP), data, fax, whether international or domestic. This does not include non-VoIP voice going over the 4ESS switches, or AT&T to AT&T (within network) communications, which would not pass through the peering links.

It Is Highly Likely That Plaintiffs' Communications Traveled Through the "Backbone"-to-Network Peering Link at the AT&T 611 Folsom Street Facility.

48. Because internet routing is so volatile, and because many email communications will be routed over temporary routes chosen by a router, it is unfathomable to me that in 17 years, at least one of plaintiffs' communications did not travel via the peering points at AT&T's 611 Folsom Street Facility, a major Internet peering point. The same is true for any other major peering point. It is thus highly likely that plaintiffs' communications traveled through the peering link at the AT&T 611 Folsom Street peering point.

49. For plaintiffs who are AT&T internet customers, it is even more likely, given that their communications would have travelled over AT&T's network so frequently. Anytime an AT&T customer sends a communication over the internet to a non-AT&T customer, that communication has to pass through a peering point with another network.

50. It is still highly likely, even for plaintiffs who were not AT&T internet customers, that their communications traveled through the peering link at the AT&T 611 Folsom Street peering point, as a function of communication with AT&T customers. Anytime a non-AT&T customer sends a communication over the internet to an AT&T customer, that communication has to pass through a peering link from another network to the AT&T network.

51. This is particularly true for individuals located in San Francisco and Los Angeles, given the high likelihood that their communications—whether to or from an AT&T customer—would be routed through the San Francisco peering link.

52. Whenever a data path develops problems (from overload, damage, equipment failure, etc.) the routers instantly compute a new path and adjust packet routing accordingly. There is potential for any traffic to pass through any node as a result of automatic temporary re-routing.

53. Real-time routing decisions are so common, and the routers are routing so many packets, that recording dynamic and temporary changes to network routing would be a burden. It is therefore not customary to keep logs or records of those dynamic re-routing decisions.

54. Routers normally do not have mass storage such as hard drives, so any record-keeping of real-time routing decisions would require sending data from the router to a logging device. This would decrease the routing capacity of the router. As a result, I am not aware of any ISP anywhere that keeps records of its dynamic routing updates—except during specific (and rare) diagnostic events.

It Is Highly Likely That The Plaintiffs' Communications Have Been Copied And Redirected By The Splitter Assemblies Described By Mr. Klein.

55. Choosing what to copy and what not to copy involves significant amounts of computing and database access. If a splitter is inserted in an internet data path, it would be very burdensome on that ISP if the computations of what to copy or not copy took place inline. The only reasonable process is to make a copy of everything and send it to an external system that would decide what to keep and what to discard. All of the communications that pass through a monitored fiber are copied and redirected. Some device then reconstitutes the individual transactions and decides which ones to keep and which ones to discard.

56. As a result, it is likely that at least one of plaintiffs' communications were copied and redirected by the splitter assemblies described by Mr. Klein, along with all of the communications passing over the peering-link fibers into which the splitters were installed. Perhaps plaintiffs' communications were not retained after they were analyzed, but they were certainly in the possession of the NSA until that analysis was completed.

(A) Mr. Klein describes a technological setup that passively copies all traffic over the peering links—not a system that monitors traffic to determine what to copy and what not to copy.

57. It is standard practice for companies that move data around as a business to purchase devices with computing resources that are a little bigger, but not a lot bigger, than they will need on the two days out of the year when they expect the most daily traffic—peak times. Monitoring and deciding whether to make a copy of a communication at that scale inside an electronic device, such as a router, would require using a significant portion of the device's computing resources, and thus throwing away the purchased computing capacity to conduct monitoring. This would cause the device to run slower, and if you didn't purchase a device with enough computing power, there would be an overload at peak times. Since no one in the industry uses routers to analyze data for monitoring, I have no source of data from which to quote numbers. However, based on knowledge of what computer chips are inside a router and what computer chips are inside a computer, I believe that it is safe to say that placing an email monitoring function inside a router would use 90% of the capacity of that router. All modern high-capacity routers perform "cut-through routing," which means that the routing decisions are made by the peripheral device controllers and not by the main router's central processing unit (CPU). Any content analysis would require disabling cut-through routing and referring all inbound traffic to the router's central computer, which by itself would cause a 50% slowdown.

58. There is significant innovation in the computer industry, and newer devices tend to be cheaper. The particular hardware and software used to copy and redirect communications transiting AT&T's peering links in Northern California and elsewhere may have changed over the years, but the factors requiring the basic architecture to copy and redirect Internet communications

transiting those peering links for further filtering and analysis is economic and not technical. Evolution in monitoring technology does not affect my conclusion that plaintiffs' communications were copied and redirected by the splitters.

(B) Monitoring "to" and "from" addressing information from an email in transit requiring first capturing and reassembling the entire email, including the message contents.

59. Monitoring the "to" and "from" addressing information in an email requires first capturing and reassembling most of the body of the email. The demarcation in an email message between its header and body is just a textual blank line, and you cannot find that blank line without assembling all of the message to that point.

60. Message assembly is done from packets, and packets typically have more than 1000 characters in them, sometimes more.

61. To find the boundary between the "to" and "from" addressing information and the body of the message it is necessary to capture as much as 1500 characters of the message payload, and these characters must correspond to part of the message that includes the "to" and "from" addressing information. The PCLOB Section 702 Report, however, states, "If a single discrete communication within an MCT [multiple communications transaction] 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."[3] This means that the NSA architecture captures and reconstitutes an entire transaction (message) before analyzing any of it, because if it did otherwise, it would not need to acquire the entire MCT once it had acquired the segment of interest. This means that the NSA has captured the entire contents of an email message even if they intend to look at its "to" and "from" addressing information.

///

///

///

///

[3] PCLOB Section 702 Report, at 39.

Conducting Surveillance at the Peering Links Between AT&T's "Internet Backbone" and Non-AT&T Internet Providers Is Consistent With Surveillance Aimed At "One-End Foreign" Communications.

62. Conducting surveillance by copying and redirecting communications in the manner described by the AT&T documents and Mr. Klein's testimony is consistent with surveillance aimed at "one-end foreign" communications transiting the "Internet backbone."

63. First, capturing the raw contents of an intercontinental fiber does not ensure that you will capture all desired communication. If you wait until other devices have merged and reassembled the fragments of the communication (some of which might have been routed over different fibers from others) you can be much more confident that you are capturing the intended communications. By the time the communications devices have merged and reassembled the fragments of international traffic into messages that can be analyzed, significant domestic traffic will necessarily have been combined with it.

64. Second, as described above, because every router involved in a message transmission makes its own decisions about the next hop in the message's journey, a router may determines that the best path for a San Francisco to Dallas transmission is to route it via Tokyo. Given that Internet service providers routinely store email message contents all over the world,[4] this is a relatively common phenomenon. Given the way information is routed over the Internet, using a splitter to copy all communications traveling across a node and then redirecting those communications in the manner described by the AT&T documents is a logical and unsurprising approach in order to ensure that all one-end foreign communications are captured. The PCLOB Section 702 Report says that the NSA conducts "technical measures, such as IP filters . . . to prevent the intentional acquisition of wholly domestic communications."[5] IP filters are only necessary because the peering links do not contain only one-end-foreign communications, but also

[4] ISPs store email messages while they wait for you to check your mail. What it means to "check your mail" is that you instruct your computer to contact the server computer on which your ISP stores your mail. ISPs do not normally reveal the location of such computers.

[5] PCLOB Section 702 Report, at 41.

wholly domestic communications. It is logical and unsurprising for such IP address filtering to occur after a splitter to copy all communications traveling across a node.

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

DATE: September 27, 2018

Brian Reid

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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 **Declaration of Professor Matthew Blaze** The Honorable Jeffrey S. White

I, Matthew Blaze, declare as follows:

1. I have been asked by counsel for plaintiffs to apply my expertise and experience to examine and analyze evidence described below. After setting forth my background, I summarize my conclusions and then explain the basis and the reasoning supporting my conclusions. If called as a witness, I could and would testify to the matters stated herein.

2. Based on my expertise, and after carefully reviewing all of the documents in this case, I believe it is highly likely that the communications of all plaintiffs passed through peering-link fibers connected to the splitter (and thus the splitter itself) that Mark Klein describes at the AT&T Folsom Street Facility. From a technical perspective, the interception architecture described in the AT&T documents and in Klein's declaration is a logical and unsurprising approach for a high-volume bulk interception operation, including interception targeting "one-end-foreign" communications.

BACKGROUND

3. I am currently employed a full professor of computer and information science at the University of Pennsylvania, in Philadelphia, where I teach graduate and undergraduate classes, conduct research, and handle various administrative matters. The focus of my research is on computer and network security, cryptography, surveillance and interception technology, and related subjects. However, I make this declaration entirely on my own behalf.

4. In 1993, I received my PhD in computer science from Princeton University. The focus of my dissertation was networking and large scale distributed systems.

5. Since 2004, I have held my current position on the faculty at the University of Pennsylvania. From 1992 through 2004, I was a member of the research staff at AT&T Laboratories in New Jersey (known for part of that period as AT&T Bell Laboratories). While at AT&T, I conducted research and led research projects in computer and network security, cryptography, surveillance and interception technology, and other topics. (I note that this declaration does not rely on any proprietary information entrusted to me during my employment at AT&T.)

6. Over the course of my career, I have produced over 100 publications related in some way to my research in computer security, networking security, cryptography, and/or surveillance. These include scholarly-refereed journal articles, refereed conference papers and workshop papers, as well as standards documents, written testimony, and articles such as op-eds in the popular press. This includes one scholarly-refereed journal articles that I co-authored with Steven M. Bellovin, Susan Landau, and Stephanie K. Pell, entitled, "It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law," published in Vol. 30 of the Harvard Journal of Law in 2016, which outlines in detail the network architecture of the Internet.[1]

7. I have been engaged as an expert in various litigation matters related to my expertise from time to time, most often in patent cases. I have testified in deposition numerous times and at trial approximately five times.

8. In addition to my professional training and conclusions, I have relied on the following information, as explained in more detail below: 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 Section 702 Report"); the Foreign Intelligence Surveillance Court order issued on October 3, 2011, for the interception of Internet content on October 3, 2011 ("FISC Oct. 3, 2011 Opinion"); the Foreign Intelligence Surveillance Court order issued on September 25, 2012, released by the government as a result of FOIA litigation with the American Civil Liberties Union ("FISC Sept. 25, 2012 Opinion"); the Classified Declaration of Deborah A. Bonanni, National Intelligence Agency Deputy Director (Dec. 20, 2013) ("NSA Deputy Dir. Fleisch Classified Decl."); the Section 702 Congressional White Paper entitled "The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act" ("FISA White Paper"); the AT&T documents attached to the Declaration of Mark Klein; the facts and events personally observed by Klein, as set forth in his declaration; and an the facts and events personally observed by James Russell, as set forth in his declaration. I do

[1] Steven M. Bellovin, Matt Blaze, Susan Landau, Stephanie K. Pell, *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016).

not rely on the conclusions Klein or Russell draw from those facts and events described in their declarations; instead I have conducted my own analysis of those facts and events.

9. I am not receiving any compensation for my work as an expert in this matter.

SUMMARY OF CONCLUSIONS

10. My conclusions can be summarized as follows:

11. First, assuming the splitter described by Mr. Klein (or similar technology) exists as described, it likely copied and redirected plaintiffs' communications.

12. Second, to extract the "to" and "from" fields from email messages transiting the Internet (what the government calls "Internet metadata") it is necessary to first acquire the entire contents of the message. This is because the "to" and "from" fields are found in the same communications layer as the content of the email message.

13. Third, conducting surveillance at the peering connections between AT&T's Internet backbone and non-AT&T Internet providers is consistent with Privacy and Civil Liberties Oversight Board (PCLOB) and Foreign Intelligence Surveillance Court (FISC) disclosures about the government's Internet surveillance.

14. Fourth, conducting surveillance at the peering connections between AT&T's Internet backbone and non-AT&T Internet providers is consistent with surveillance aimed at "one-end foreign" communications.

EXPLANATION OF THE BASIS FOR MY CONCLUSIONS

How Communications Travel On The Internet

15. The Internet is a packet-switching network. That means that communications are broken into small packets, each of which may be routed a different way through the communications network. The packets are then reassembled at the communications endpoint, where they are received as, for example, an email, video, or webpage.

16. In the conventional description, computer network technology is organized as a "stack." From the bottom down, the "layers" are physical, link (or data link), network, transport, and application. The layer names come from the reference architecture of the Open Systems Interconnection (OSI) standard. The layers are often referred to by number, rather than by name

(e.g., the physical layer is "layer 1"; the link layer is "layer 2"; and so on). Though the OSI protocols, which predate the Internet, are now largely defunct, the terminology has lived on even though it is not a perfect match for today's Internet architecture. For example, while the OSI standards included 7 layers, two additional layers than those listed above, on the internet there are no equivalents to OSI layers 5 (a session layer) and 6 (a presentation layer); some of the layer 6 functionality, however, often appears as part of layer 7 (the application layer). Given the history behind the development of modern day internet networking standards, there continues debate amongst network engineers about the precise number of layers to include in descriptions of how information travels across the Internet and the precise terminology used to describe these layers, but the functionality remains the same.

17. Each layer in the stack offers a specific set of services (provided via software) to the layer immediately above it, and requests services from the layer below it. As information travels across the Internet, these services are typically carried out via a string of digital devices: a layer on one device talks to the corresponding layer on the next device. These services are not provided in the network but on the "edges." Data in the application layer (OSI layer 7), and transport layer (OSI layer 4) are not processed by intermediate routers in the Internet. The communications in the application and transport layers are end-to-end communications from Host A (the originating or "source" computer) to Host B (the receiving or "destination" computer). For example, web servers and email servers are not generally part of the Internet infrastructure itself, but rather are provided by ordinary computers at the "edge" of the Internet, generally operated parties other than the ISP.

18. Different protocols govern the communications between layers and between devices on the same layer.

19. The top layer, the application layer, supports application and end-user processes. The application layer provides the basis for e-mail forwarding and storage. It allows a user to pass information to a network. For example, the software application that you type an email into using your computer and the software application displaying it on the other end function at the application layer. The application layer uses a variety of different protocols.

20. The transport layer accepts data from the application layer, splits it up into smaller units, passes these data units (also called "packets" or "datagrams") to the network layer, and ensures that all the pieces arrive at the other end. It also reassembled packets on the other end by putting data back together in the correct order. These services are conducted via the Transmission Control Protocol ("TCP"). TCP, for example, will retransmits any packets are dropped by the next layer, the network layer, during transmission to ensure that all packets necessary to reconstruct the data sent arrive at the destination computer. At the transport layer, a packet includes a TCP header, which includes a port numbers, which act as the internal address within the destination computer. It is fundamental to the design of the Internet that TCP headers are end-to-end; they are not processed by intermediate routers in a network. This means that the contents of the TCP header are created by one end system and are relevant only to the computer at the other end of the connection. Unlike the network layer, intermediate routers do not ordinarily examine or otherwise rely on TCP headers. In other words, the data transmitted with TCP and in the TCP header is not, from an Internet design perspective, shared with other parties. The only true party to TCP communications is the destination computer at the other end of the connection. As far as the network is concerned, TCP headers are just unexamined content.

21. The network layer accepts packets from the transport layer and routes and delivers those packets from source to destination across multiple networks. Gateways—such as router, firewall, server, or others device that enables traffic to flow in and out of a network—function at the network layer. The network layer uses the Internet Protocol ("IP") to route and deliver packets. At the network layer, each packet includes a "header" that describes what the packet is, along with where the packet is going and where it came from, in the form of Internet Protocol addresses (or "IP addresses). Whereas a port number more or less is similar to a room in a building, an IP address is similar to the building's address.

22. The information contained within packet headers—whether the IP header or the TCP header—is distinct from the "to," "from," and "subject line" information contained within an email. The "to," "from," and "subject line" information of an email can be viewed only at the application layer, *after* packets are reassembled via TCP/transport level. As a result, IP-based

communications render content/non-content distinctions in email functionally meaningless. Networks—and specifically, the routers and the links that connect them—are concerned solely with packet delivery from a source IP address to a destination IP address, and not the contents of the packet.

23. The link, or data link, layer provides the protocol mechanisms needed to send and receive packets on a single network. The link layer first forms "frames" (or protocol data units") from the packets it receives from the network layer and sequentially transmits the frames to the physical layer. The link layer creates frames by dividing the streams of bits received from the network layer into manageable data units, typically a few hundred or few thousand bytes. The link layer then transfers these frames between adjacent network nodes (or "peering links") in a wide area network (WAN), a computer network that extends over a large geographical distance/place, or between nodes on the same local area network (LAN) segment, a computer network that interconnects computers within a limited area such as a residence, university campus, or courthouse, such as a Wi-Fi or Ethernet. Each frame has a header, describing, for example, the source Ethernet address and the destination Ethernet address. (Just as with IP and TCP headers, the information contained within a frame header is completely distinct from the "to," "from," and "subject line" information contained within an email.) The receiver typically confirms correct of each frame by sending back an acknowledgement frame.

24. The lowest layer of the stack, the physical layer, cover the physics of communication: the radio frequencies used, the voltages for traditional Ethernet, the electrical or optical properties of the physical connection between a device and the network or between network devices, and more. This layer has no concern for the meaning of the bits; it deals only with the setup of physical connection to the network and with transmission and reception of signals.

25. On the receiving end, the reverse happens. The physical layer provides bits to the link layer, which reconstructs packets via frames. The network layer accepts the packets from the link layer, and then, using the IP address information contained with the packet header, routes and delivers those packets to the destination address. The transport layer, via TCP, accepts the packets

and reassembled them, putting the data together in the correct order so that it may be displayed in human-readable form via the application layer.

26. Internet Service Providers (ISPs) provide service at the Network Layer discussed above by routing the packets to their destinations. All Internet service providers, including AT&T, route traffic for variety of parties, including the inbound and outbound traffic for their own customers coming from or going to other computers on the Internet connected to other ISPs. AT&T also serves as what is known as a "backbone" provider, handling traffic not only for its own customers, but also "transit" traffic passing between other Internet service providers. It is through large backbone providers such as AT&T that local Internet service providers are able to connect their customers to the entirety of the Internet. The effect is that the packets passing within AT&T's network (including in the San Francisco office) will include three kinds of traffic: that being routed between two AT&T customers, that being routed between AT&T customers and those of other ISPs, and that being routed between one ISP and another ISP. All three kinds of traffic would be expected to have been included on split links sent to the NSA room in the San Francisco office.

Given The Inherent Structure Of The Internet, Collecting "To" And "From" Addressing Information From Emails In Transit Requires Capturing All The Packets Related To The Email And Reassembling The Entire Email.

27. Given the inherent structure of the Internet outlined above, there is no way to view or collect the "to" and "from" addressing information from an email messages by packet interception without first reconstructing the email message content by reassembling the contents of all of the relevant packets.

28. The outdated conception of a bright line between content and addressing information (which is sometimes referred to as "metadata") originates from early phone networks. Originally, metadata was a reference to the dialing, routing, addressing, and signaling (DRAS) information utilized in the Public Switched Telephone Network (or "PSTN").

29. Unlike the Internet, which is a packet-switched network, the traditional telephone network is a circuit-switched network, in which each communication builds a circuit that it uses exclusively for the duration of a call. And unlike the Internet's architecture, where the intelligence

is at the edges (in the connected computers, rather than in the network itself), in the phone network, the intelligence is centralized in the telephone company's infrastructure: the phone switches. As the only elements of that network with any sophistication, the phone switches must receive and process all signaling information (encoded as tones or dial pulses) to complete calls. At the time of the development of the telephone network, this design was a practical necessity: the phones of the time were very simple devices with no computing or storage capability, and rotary dial phones were almost completely electromechanical save for a few passive electronic components.

30. The essential architecture of the phone network was designed at a time when putting any but the most basic functions in telephones was technically and economically infeasible. The phone network's design meant that most services had to be provided by the telephone companies, and the phone companies could offer only rudimentary services to their customers—notably dialing or answering a phone call. Requesting a service was easy: you took the phone off the hook and listened for a dial tone. You then dialed the number and the phone system (rather than the user's phone) would do all the subsequent work needed to complete the call.

31. Given the rudimentary communications model of the phone network, it was plausible for the courts to draw a bright line between content (a conversation, or perhaps a modem session) and metadata (DRAS information). Even by 1979, however, as advanced features started to appear in the phone network, the line content and addressing information began to blur.

32. IP-based communications, in contrast, render the content/non-content distinctions functionally far less meaningful.

33. For example, in the phone system, "addressing" is straightforward: it is the task of specifying to the network the destination of a call, and an "address" is "a unique 10-digit number assigned to a main station, *i.e.*, a phone number. On the Internet, the link, network, transport, and application layers all have their own identifiers—and none of these identifiers include the email address listed in the "to" or "from" fields in an email. From a technical perspective, the "to" and "from" information, along with the subject line and the text within the body email, is *all* content information, because, as described above, it can only be viewed at the application layer, after content has been extracted and reassembled from the packets.

It Is Likely That The Plaintiffs' Communications Have Been Copied And Redirected By The Splitter Assemblies Described By Mr. Klein.

34. As noted above, the Internet backbone is a complex network of communication links over which traffic is routed. A "splitter," as used in this case, is a device that optically "splits" all communication on a link between two network nodes, creating an second link that can be connected to a third node. This effectively copies all the traffic on the original link to the third node, while leaving the traffic undisturbed between the original two nodes. It is, in effect, a specialized device for physically "wiretapping" the kinds of high-speed optical communication links that make up the Internet backbone.

35. Klein testifies he personally observed and operated the splitter, and for purposes of this analysis I accept his description of how the splitters operated, what peering-link fibers they were connected to, and that the copied, as these are all facts within his personal knowledge and observation. I do not rely on any further conclusions Mr. Klein drew from those facts he observed; instead, I analyze those facts independently.

36. I independently analyze the AT&T documents and do not rely on Klein's description of them. I accept AT&T Director of Asset Protection Russell's testimony that they are authentic AT&T documents.

37. The system described by the AT&T documents and Klein's personal observations does the following: "Taps," via splitters, backbone communication links in the AT&T San Francisco facility, routing a copy of the traffic on these links to a secure room controlled by the National Security Agency (NSA).

38. From a technical perspective—given that extracting the "to," "from," subject line, and text within the body of emails requires reconstructing all packets that comprise an email—this interception architecture, in which all the traffic passing across peering-link fibers is copied via a splitter and then filtered separately, is a logical and unsurprising approach for a high-volume bulk interception operation. An alternative approach would involve scanning for and copying the desired traffic in the ISP's routing infrastructure itself. But such an approach would require significant changes on the part of the ISP, and could potentially degrade the ISP's performance,

especially when large volumes of traffic are to be intercepted. Another approach (common used for lawful interception of email by law enforcement) would dispense with the need for any packet interception by obtaining the data from the operators of the targeted users' mail servers. However, this approach requires the active cooperation of the various mail server operators, many of which, for international users, are located outside the jurisdiction of the United States.

39. It is highly likely that the communications of all plaintiffs passed through the link connected to the splitter (and thus the splitter itself) that Klein describes.

40. As the Internet "routes" communications through the network, the particular links through which a packet travels to its destination is a function of the state of the network at the precise instant a packet is sent, rather than an attribute of a particular connection.

41. It is my understanding based on the available evidence that the AT&T San Francisco peering-link fibers to which the splitter was attached carried a high concentration of the international and domestic Internet traffic passing through the AT&T San Francisco facility. That means that the link connected to the splitter would, in turn, have access to a large fraction of the traffic passing through the facility. This would include Internet traffic of AT&T's customers—including traffic of plaintiffs who are AT&T Internet customers—as well as peering traffic of customers of other ISPs who communicate online with AT&T customers.

42. Pursuant to the inherent architecture of the Internet, in order for a communication from an AT&T customer to reach a non-AT&T customer, that communication has to pass through a peering point with another network. Likewise, a communication from a non-AT&T customer to an AT&T customer must has to pass through a peering point with another network.

43. For those plaintiffs who are AT&T Internet customers, there is even more of a likelihood that their communications passed through the node connected to the splitter (and thus the splitter itself) that Klein describes, given that they would have been on AT&T's network so frequently. But it still highly likely that plaintiffs' communications passed through the link connected to the splitter (and thus the splitter itself) that Klein describes, even if they were not AT&T Internet customers, as a result of communicating with AT&T customers.

44. The fact that all plaintiffs reside in either northern California or southern California also increases the likelihood that their communications passed through the node connected to the splitter (and thus the splitter itself) at the AT&T San Francisco facility, given the proximity of the San Francisco peering site and the high concentration of the international and domestic Internet traffic passing through it.

45. The AT&T documents also suggest that there are similar splitter systems at other AT&T facilities. If that is true, then that would only increase the odds that plaintiffs' communications passed through peering-link fibers to which splitters were installed at AT&T peering points.

46. It would not be surprising if the particular hardware and software used to copy and redirect communications transiting AT&T's peering links in Northern California and elsewhere has changed over the years. But as long as the basic architecture copies and redirects Internet communications transiting those peering links for further filtering and analysis, my conclusion that plaintiffs' communications are likely subject to the initial copying and redirection remains valid.

Copying And Redirection Of Plaintiffs' Communications At AT&T's Peering Links Is Consistent With The PCLOB's Description And Other Government Disclosures Of The NSA's Interception Of Internet Content For Purposes Of Selector Searching.

47. The use of splitters or similar technology to copy and redirect communications transiting Internet backbone peering links as disclosed by the AT&T documents and Klein's testimony is consistent with the disclosures by the Privacy and Civil Liberties Oversight Board (PCLOB). The PCLOB states that the government's interceptions occur "with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit." PCLOB Section 702 Report, at 7.

48. The PCLOB further states:

a. The NSA "intercepts communications directly from the Internet 'backbone.'" *Id*. at 124.

b. The interceptions are of "communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the 'Internet backbone.'

The provider is compelled to assist the government in acquiring communications across these circuits." *Id*. at 36-37.

c. "The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet." *Id*. at 39.

d. "[U]pstream collection acquires 'Internet transactions,' meaning packets of data that traverse the Internet, directly from the Internet 'backbone.'"

e. The interceptions occur "in the flow of communications between communication service providers." *Id*. at 35. That is a description of "peering links."

49. Other government disclosures also confirm that interceptions of Internet backbone communications are occurring: "[T]he NSA collects electronic communications with the compelled assistance of electronic communications service providers as they transit Internet 'backbone' facilities within the United States." NSA Deputy Dir. Fleisch Classified Decl., at 25. "NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States." FISA White Paper, at 3.

50. The Foreign Intelligence Surveillance Court (FISC), similarly confirms "the acquisition of Internet communications as they transit the 'internet backbone' facilities[.]" FISC Sept. 25, 2012 Opinion, at 26.

51. These descriptions are consistent with the splitters described by the AT&T documents and Klein that copy and redirect communications transiting peering links between AT&T's backbone and other Internet providers.

Conducting Surveillance At The Peering Connections Between AT&T's Internet Backbone And Non-AT&T Internet Providers Is Consistent With Surveillance Aimed At "One-End Foreign" Communications.

52. Conducting surveillance by copying and redirecting communications in the manner described by the AT&T documents and Klein's testimony is consistent with surveillance aimed at "one-end foreign" communications transiting the Internet backbone.

53. The PCLOB states: "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

communications, what is referred to as the 'Internet backbone.' 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." PCLOB Section 702 Report, at 36–37.

54. The PCLOB further states that the NSA uses "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." PCLOB 702 Report, at 38. The NSA employs these "technical measures, such as IP filters . . . to prevent the intentional acquisition of wholly domestic communications." *Id*. at 41.

55. IP filters are necessary only because the communications links the government monitors *do* contain wholly domestic communications, in addition to one-end-foreign communications. Otherwise they would not need to be filtered out.

56. From a technical perspective, the interception architecture described in the AT&T documents and Klein declaration is consistent with the NSA's goal of conducting surveillance on "one-end foreign" communications, because use of a splitter to copy all communications traveling across a node ensures that all one-end foreign communications are captured, so that the NSA may then conduct IP filtering. IP filtering at other places in the network itself would likely degrade the ISP's performance.

57. Further evidence that the communications links the government monitors do contain wholly domestic communications is the fact that, as the FISC has noted, "NSA's upstream collection devices will acquire a wholly domestic 'about' [communication] if it is routed internationally." FISC Oct. 3, 2011, at 34.

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

DATE: September 28, 2018

Matthew Blaze

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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 **Declaration of Ashkan Soltani** The Honorable Jeffrey S. White

I, Ashkan Soltani, declare as follows:

1. I have been asked by plaintiffs' counsel to apply my expertise and experience to examine and analyze the evidence described below. In this declaration, I set forth my background, summarize my conclusions, and explain the basis and the reasoning supporting my conclusions. If called as a witness, I could and would testify to the matters stated herein.

2. Based on my expertise and experience, and after reviewing documents in this case, plaintiffs' use of cloud-based services such as webmail like Google's Gmail and Yahoo email increases the likelihood that their communications would be subject to collection as part of a surveillance network such as the one described by plaintiffs, even if that network were intended to intercept only communications with an international nexus.

BACKGROUND

3. I am a technology researcher and consultant with a focus on matters of privacy, cybersecurity, and policy. I have 20 years of experience in industry, government, and media, including work at the White House, Federal Trade Commission (FTC), Washington Post, and Wall Street Journal. Among other honors, my work as a co-author of the Washington Post's series on the National Security Agency (NSA) was awarded the 2014 Pulitzer Prize for Public Service.

4. I am currently the principal at Soltani, LLC, where since 2012 I have acted as a court-recognized technology expert and provide research, analysis, forensics, and testimony for clients such as the FTC and Attorneys General of California, New Jersey, Tennessee, and Ohio.

5. I received a Bachelor of Science degree in Cognitive Science with a minor in Computer Science from the University of California, San Diego in 1998. My studies focused on learning algorithms, collaboration, and data mining.

6. Between 1999 and 2005, I was a professional services consultant at Sophos, Inc. I consulted on network security and architecture for clients such as AT&T, Bank of America, Cisco, Amazon.com, NTT Japan, and the US Department of Homeland Security.

7. I received a Master of Information Management and Systems degree from the University of California, Berkeley in 2009.

8. My master's thesis, *KnowPrivacy*: *The Current State of Web Privacy, Data*

Collection, and Information Sharing, led me to serve as a consultant and investigative reporter for the Wall Street Journal's *What They Know* series, which examined the state of online tracking. I developed methods and tools to identify tracking technologies and their use, including demonstrating evidence of price discrimination online. The *What They Know* series was a finalist for the 2009 Pulitzer Prize for Investigative Reporting.

9. Between 2013 and 2014, I was the co-author of a series of articles documenting the extent of the NSA's surveillance programs for the Washington Post. The series was awarded the 2014 Pulitzer Prize for Public Service, the 2014 Loeb Award, and a 2013 Polk Award for National Security Reporting.

10. In 2010, I served as one of the first staff technologists at the FTC's Privacy and Identity Protection division. I conducted investigations into online security and privacy matters, including behavioral advertising, online tracking, and mobile privacy. I also assisted Commission staff in data gathering and forensics, analysis, reports, access letters, subpoenas, complaints and consent agreements on cases including Twitter, Google, Facebook, Myspace, and HTC.

11. Between 2014 and 2015, I served as the Chief Technologist at the FTC, where I was responsible for guiding the Commission on technology policy issues relating to privacy, security, and consumer protection. I created and staffed a new Office of Technology Research and Investigation to lead the agency's technical efforts.

12. Between 2015 and 2016, I was a Senior Advisor at the White House Office of Science and Technology Policy (OSTP). Serving under the White House Chief Technology Officer, I was responsible for developing United States policy on emerging technology issues including privacy, artificial intelligence, and big data.

13. The conclusions that I draw below rely on my professional training and experience, in addition to the following information, as explained in more detail below: documents and interviews I reviewed while reporting on the NSA for the Washington Post, and documents published by Google and Yahoo.

14. I am not receiving any compensation for my work as an expert in this matter.

SUMMARY OF CONCLUSION

15. My conclusion can be summarized as follows:

16. Plaintiffs' use of cloud-based applications, such as webmail like Google's Gmail and Yahoo email, increases the likelihood that their communications would be subject to collection as part of a surveillance network such as the one described by plaintiffs. For reasons related to availability, including disaster avoidance and server load, users' communications and associated data, including email accounts, are rarely stored in a single data center but often span across multiple, redundant geographic data centers. A single draft email message, even prior to it being sent, may be copied across multiple disparate computing systems in case an outage occurs at any single instance. As such, the distribution of emails between these data centers happens frequently and does not require that users send or receive email—and this distribution is designed specifically to traverse geographic borders in order to provide geographic redundancy. Therefore, even if defendants' Internet surveillance collection points are designed primarily to collect Internet traffic on foreign links or communications that originate or terminate outside the United States, it is likely that data belonging to users of cloud-based applications such as cloud email services passes through these collection points.

EXPLANATION OF THE BASIS FOR MY CONCLUSION

Large Providers of Cloud-Based Applications Store Data Such as the Contents of User Email Accounts Data Centers Located Around the World

17. As providers of cloud-based applications have grown larger, they have developed sophisticated systems to store and retrieve data including the contents of user email accounts.

18. A seminal paper published by Google in 2012 describes how one of these systems, a database named "Spanner," operates.[1] Spanner serves Google's goal of ensuring that data in the database has "high availability" and "low latency," that is, data is rarely if ever inaccessible, even in the face of failure of entire data centers, and that it can be retrieved and delivered to an end user with a minimum of delay. Spanner accomplishes these goals by breaking up data into segments or

[1] Google, *Spanner: Google's Globally-Distributed Database* (2012), https://static.googleusercontent.com/media/research.google.com/en//archive/spanner-osdi2012.pdf ("Spanner paper").

"shards," which it moves dynamically between Google data centers. It relies on distributed atomic clocks and GPS sensors to synchronize the movement of shards at a highly precise time scale, allowing changes to be made rapidly to the same set of data at different places in Google's network without leading to inconsistencies.

19. Data "shards" in the context of Google Spanner are not to be confused with IP "packets," which are the basic network data blocks in computer networking. Depending on the specific configuration, each "shard" may include significant portions of content, including email messages, chat conversations, and attachments. If the NSA or other outsiders intercepted a single shard, they could glean significant information about the communications, including an entire email or chat. Even if a shard did not contain a complete communication, interception of multiple shards would allow the entire communication to be reconstituted.

20. As a result, the location of individual shards in these data centers frequently changes. For example, "Spanner automatically reshards data across machines as the amount of data or the number of servers changes, and it automatically migrates data across machines (even across datacenters) to balance load and in response to failures."[2]

21. Spanner is used to manage the distribution of Google's Apps, including its Gmail email service. Therefore, shards of Google Apps user data, including the contents of Gmail users' accounts, are moved frequently between Google data centers as Spanner manages load on Google's network and ensures the availability of this data.

22. Google operates approximately 15 data centers located in North and South America, Europe and Asia.[3]

23. Yahoo operates similar databases to Spanner to manage and distribute data including the contents of email accounts among its global data centers.

24. Therefore, an email message belonging to a user of a cloud-based email service may move frequently between locations around the world even without action by the user.

---

[2] Spanner paper at 1.
[3] *See* Google, *Data center locations*, https://www.google.com/about/datacenters/inside/locations/index.html.

25. Due to the dynamic nature of Spanner and similar databases employed by Yahoo, it is likely that a program designed to conduct surveillance on the Internet backbone, even one aimed specifically at foreign Internet links or communications between individuals outside the United States would result in the collection of even purely domestic communications belonging to American users of cloud-based applications located in the United States.

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

DATE: September 28, 2018

Ashkan Soltani

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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.: 4:08-cv-4373-JSW **DECLARATION OF CAROLYN JEWEL IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** September 28, 2018 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. Attached at the end of this declaration is a table describing the various Internet and phone services to which I have subscribed, along with a list of other Internet-based services, platforms, and communications tools I use in my personal and professional capacities. A summary of those activities is included below.

Internet Service and Use

3. I have received Internet service from various services provided by AT&T since 2000.

4. I began receiving Internet service from AT&T in 2000 when I subscribed to its Worldnet dial-up service, which I used until 2009.

5. Between 2010 and 2015, I subscribed to multiple AT&T data plans using Hot Spot wireless or tethering Internet services. I currently subscribe to AT&T's U-Verse Internet service, which I began using in 2015.

6. I also subscribed to a number of other Internet service providers not affilited with AT&T between 2008 and 2015. This included a subscription to WildBlue Satellite Internet service from 2008 to 2011 and Millenicom Wireless between 2011 and 2014.

7. I used my AT&T and other Internet subscriptions 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.

8. I use my AT&T and other Internet services to send correspondence and engage in activities that I expected 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.

9. 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, for my novel *A Darker Crimson*, published in 2005, I researched rail guns and other similar weaponry. I published a historical romance novel in 2009 titled *Indiscreet*, which was set in Turkey and Syria, for which I did significant research on foreign websites about those countries. For the *My Immortals* series of novels, the first novel of which was published in 2008 and the most recent in 2016, I researched the history and folklore of demons and other supernatural beings in countries across the word. For several novels I have researched the use of various types of historical and modern weapons, 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.

10. 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.

Website Operations

11. I operate a number of websites for in both personal and artistic capacities. For example, I have operated the domain www.carolynjewel.com since 2000. The website provides inforamtion about me, the books I've written, writing tips, a calendar of upcoming appearances, and the ability to subscribe to my newsletter.

12. For my work as a writer, I also operate https://cjewelbooks.com/, which allows visitors to purchase all of my books. I've operated the website since 2017.

13. I also operate www.cjewel.com for personal purposes, including hosting a blog I write. I've operated the website since 1999.

14. I have been using http://cjewel.me since 2013 to run a custom link-shortening service that allows me to create short links to content, including links in my ebooks.

Email Communications

15. I use multiple email accounts daily for both professional and personal purposes.

16. For example, I use accounts through AT&T, my websites, and other email providers to engage 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 review 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.

Additional Internet activities

17. I regularly use social media and other Internet services, particularly for my work as an author.

18. For example, I use social media services such as Twitter and Facebook to announce forthcoming novels, interact with readers, and connect with family and friends. Being active and responsive on these platforms is essential to my work as a published author.

19. I am on multiple email loops and/or groups that deal with the subject and business of writing, including several Yahoo groups as well as and email forms hosted by Romance Writers of America (RWA). Yahoo and RWA related forum emails are routed to me through my email address associated with www.carolynjewel.com. I have been a member of RWA's National Board of Directors since 2014. For the years 2018-2020, I will be RWA's President-Elect and then President. RWA Board related emails frequently contain matters of a highly sensitive and confidential nature. I am also on a Google group related to Microsoft SQL Server database administration. This Google group was originaly an email forum provided by a now-defunct website called LazyDBA. Currently, those emails route through my gmail address and are forwarded to my email address provided by my employer.

20. I also use online communications services such as Skype and Google's chat service, Gchat. I have used Skype to talk with friends, family, and colleagues since 2012.

21. I also regularly use other online services in both my personal and professional capacities. For example I use online file storage and transfer services such as Dropbox and WeTransfer.

Phone Services and Use

22. My family has had residential phone service through AT&T since 1966. I currently subscribe to AT&T's Internet phone service and use the same number that my parents first used.

23. I currently subscribe to cellular phone service through AT&T, and have used their service since 1999. I also previously subscribed to Virgin Mobile's cellular phone service via a mobile hot spot from 2013 to 2015.

24. I also use Google's online phone service, Google Voice, and have since 2006.

25. I have used my residential and cellular phone services to send and receive phone calls as part of my professional and personal life. I have always expected that these calls, including information about who and when I make and receive calls, to remain private.

26. I also rely on my cellular phone service's data network, through AT&T, to access the Internet. I use this Internet access in ways similar to my use of my residential Internet service as described above. I also use my AT&T cellular phone service to communicate with friends, family, fans, and colleagues through online messaging services.

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

Executed on September 25, 2018 at Petaluma, California.

CAROLYN JEWEL

Plaintiff Carolyn Jewel's
Communication and Internet Services

Type of service	Name of Provider/Service	Beginning date	End Date
Internet Service	AT&T U-Verse	2015	Present
	AT&T Wireless data	2010	2015
	AT&T Hot Spot Wireless	2010	2015
	AT&T dial-up Internet	2000	2009
	WildBlue Satellite Internet	2008	2011
	Millenicom Wireless	2011	2014
	Virgin Mobile Wireless	2013	2015
	Blue Mountain Wireless	2014	2014
Residential Phone	AT&T	1966	Present
	Google Voice	2006	Present
Cellular Phone	AT&T	1999	Present
	Virgin Mobile	2013	2015
Websites	www.carolynjewel.com	May 2000	Present
	www.cjewel.com	May 1999	Present
	www.cjewelbooks.com	2017	Present
	www.cjewel.me	August 2013	Present
Email	Account through AT&T	August 2015	Present
	Account through Yahoo	January 2000	Present
	Accounts through Google's Gmail	August 2004	Present
	Account through Protonmail	January 2017	Present
	Accounts through Hushmail	July 2014	Present
	Accounts through websites such as www.carolynjewel.com	May 2000	Present
	Account through WildBlue Internet service	2008	2011
	Accounts through Amazon Kindle	2007	Present
	Accounts through LegacyNet	2000	Present
	Account through Nelson HR	2006	2012
	Account through Zerochaos	2012	2015
Social Media	Twitter (multiple accounts)	March 2007	Present
	Facebook (multiple accounts)	2010	Present
	Pinterest	2012	Present
	LinkedIn	2007	Present
	Instagram	2015	Present
	Mastodon	2017	Present
	Discord	March 2017	Present
	Slashdot	2005	Present
	Reddit	2016	Present
	Tumblr	2013	Present
	Snapchat	2015	Present
	Ello	2014	Present
	Tsu	2014	Present
	MySpace	2004	2013
	Friendster	2004	2015

Other Online Services	Microsoft online services	2013	Present
	Amazon Web Services	September 2014	Present
	Wattpad	June 2010	Present
	Atlassian (Jira software)	2013	2015
	Metafilter	December 2014	Present
	Kboards.com (forum)	February 2014	Present
	Skype	2012	Present
	Google Gchat	2008	Present
	Amazon Chime	2017	Present
	Blab	2015	Present
	Pokemon Go	July 2016	Present
	Dropbox	2010	Present
	Apple iCloud	June 2016	Present
	Github	September 2013	Present
	WeTransfer	2012	Present

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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.: 4:08-cv-4373-JSW **DECLARATION OF TASH HEPTING IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** September 28, 2018 Courtroom 5, Second Floor The Honorable Jeffrey S. White

I, Tash Hepting, hereby declare:

1. I am a plaintiff in this action, and I reside in Livermore CA. Prior to that, I resided in San Jose, CA. I am a Technical Marketing Director in San Jose CA, and prior to that I have held various other technical positions in the networking industry over the last 25 years including Systems Architect, Technical Support Escalations, and Software Quality Assurance.

2. Attached at the end of this declaration is a table describing the various Internet and phone services to which I have subscribed, along with a list of other Internet-based services, platforms, and communications tools I use in my personal and professional capacities. A summary of those activities is included below.

Internet Service and Use

3. I currently receive Internet access at my home from a subscription to Comcast. I have been a subscriber to Comcast since 2010.

4. Previously, I received Internet access through a subscription from Speakeasy.net from 2001 to 2009.

5. I have relied on my Comcast, and before that, Speakeasy.net, Internet service for a variety of activities, including sending and receving private messages to family, friends, and professional colleagues, browsing the Internet, shopping, banking, and playing games. For all of these activities, which were done in both professional and personal contexts, I expected them to remain private.

6. Using the Internet is particularly important to me because it facilitates a number of personal and professional uses including transmission of confidential and/or proprietary information, communication and collaboration with industry colleagues, private communications with family/friends over chat/voice/video, gaming and other entertainment, streaming video and music from services like Netflix, educational resources, sharing photos, and numerous other uses as part of my daily life. For family, friends, work colleagues, and customers who are international, the Internet is the primary (and frequently only) method of communication that is practical and affordable.

Website Operations

7. I operate several websites such as www.hepting.com, www.hepting.org, www.slipshod.net, www.hepting.net for personal use and have since 1996.

8. For example, I have ran the domain www.hepting.com since December 1996. I use this domain to provide email for myself and for my family, as well as to learn various web technologies and in the past to host photographs of portrait sessions I had done with friends and family.

9. I also continue to operate www.hepting.org, which I have used since September 2000, and www.hepting.net, which I began in March 2001. I use these domains to maintain my online presence and to prevent malicious use of my name.

Email Communications

10. I have several email addresses that I use to communicate online in both my professional and personal capacities.

11. For example, I have multiple email addresses set up through my website domains such as www.hepting.com and www.hepting.org that I use for email correspondence with businesses, friends, and family in both the US and various international locations.

12. I also have email addresses through Google's Gmail services, which I first began using in 2007.

13. I also have an email address through my employer, Zscaler

Additional Internet activities

14. I use a variety of other online services for work and pleasure.

15. For example, I use file-sharing, storage, and collaboration services such as Dropbox, Google Drive, and Microsoft OneDrive for backups of personal files, exchanging files with friends and colleagues, and for storing confidential and proprietary files of my employer.

16. I also make use of online gaming services such as Steam and Xbox Live that allow me to play games with others online who may or may not be located within the US.

17. I also make use of online encrypted chat services like Telegram and Google Hangouts to maintain a close relationship with teammates in a gaming community that coordinates play for a

global location-based "capture the flag" style game named "Ingress." At times I have been in group chats with teammates from countries across 5 continents, exchanging private communications about game strategy, directing game participants, or distributing proprietary & confidential content for use by our team.

Phone Services and Use

18. I have received residential phone service from AT&T since 2001.

19. I currently receive cellular phone service from T-Mobile and have since 2015.

20. I previously subscribed to Verizon Wireless, including having multiple lines on my subscribtion, from 2001 until 2017.

21. I also currently receive phone service through Google Voice, a web-based service that I have used since at least late 2009.

22. I have relied on both my residential, cellular, and Google Voice phone services to send and receive phone calls of both a personal and professional nature. I have always expected that these communications, and the fact that I made or received calls, to remain private. While I was in Technical Support, I would frequently make and receive international phone calls to work colleagues, and occaisionally to international customers located in Canada, Europe, and Isreal.

23. I have also relied on my cellular phone services' data networks to access the Internet and use phone-based applications, or apps, for a variety of purposes, such as messaging friends and co-workers, shopping, and banking.

24. Just as I rely on my residential Internet service for my professional endeavours, I similarly use my cellular services' data networks to facilitate access to private and/or confidential documents, corporate applications and resources, and private and professional communications over text/voice/video. While this access has primarily been conducted from within the US, I also utilize this service when I am traveling internationally for personal or business trips.

/

/

/

/

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on September 27, 2018 at Livermore, California.

TASH HEPTING

Communication and Internet Services

Type of service	Name of Provider/Service	Beginning date	End Date
Internet Service	Comcast	2010	Present
	Speakeasy.net	2001	2009
Residential Phone	AT&T	2001	Present
	Google Voice	2009	Present
Cellular Phone	Verizon Wireless	2001	2017
	T-Mobile	2015	Present
Websites	www.hepting.org	September 2000	Present
	www.hepting.com	December 1996	Present
	www.hepting.net	March 2001	Present
	www.slipshod.net	June 2002	Present
Email	Accounts through www.hepting.com	1996	Present
	Accounts through www.hepting.org	2000	Present
	Account through employer Zscaler	April 2017	Present
	Accounts through Google's Gmail	2007	Present
Social Media	Twitter	June 2007	Present
	Facebook	January 2009	Present
Online Communication	Google Chat	2007	Present
	Telegram	September 2014	Present
	Facebook Messenger	August 2011	Present
Other Online Services	Dropbox	August 2013	Present
	Box	August 2013	Present
	Flickr	2006	Present
	Steam (online gaming platform)	November 2004	Present
	Xbox Live	April 2006	Present
	Sugarsync	February 2013	May 2017
	Microsoft OneDrive	April 2013	Present
	Google Drive	January 2010	Present

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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.: 4:08-cv-4373-JSW **DECLARATION OF YOUNG BOON HICKS IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** September 28, 2018 Courtroom 5, Second Floor The Honorable Jeffrey S. White

I, Young Boon Hicks, hereby declare:

1. I am the widow of Gregory Hicks and executrix of the estate of Gregory Hicks, a plaintiff in this action who died in September 2010. After Mr. Hicks' death, I was substituted as executrix as a party to the damages claims in this action. (ECF Nos. 124, 125).

2. Mr. Hicks resided in San Jose, Californa from 1995 until his death in September 2010.

3. After reviewing the available records of Mr. Hicks' telelphone and Internet usage, I am informed and believe the following:

4. Mr. Hicks was the named subscriber of residential phone service from AT&T from February 1995 to December 2010, and I became the named subscriber thereafter.

5. Mr. Hicks was the named subscriber of cellular phone service from Sprint from March 2006 to December 2010, and I became the named subscriber thereafter.

6. Mr. Hicks was the named subscriber of Internet service from Comcast from 2008 to 2010, and I became the named subscriber thereafter.

7. Prerviously, Mr. Hicks was a subscriber of Internet service from AT&T from 2006 until 2008.

8. Mr. Hicks had at least two e-mail accounts that he regularly used. He used one, at the domain cadence.com, from at least 2002 to 2010. He used the second, at the domain hicks-net.net, from at least April 2007 to 2010.

9. Mr. Hicks also operated his own domain on the World Wide Web, www.hicks-net.net. The doman was active from April 2007 to April 2013, as it remained online after Mr. Hicks' death.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge, information, and belief. Executed on September 20, 2018 at Mountain View, California.

Young Boon Hicks

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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.: 4:08-cv-4373-JSW **DECLARATION OF ERIK KNUTZEN IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** September 28, 2018 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. Attached at the end of this declaration is a table describing the various Internet and phone services to which I have subscribed, along with a list of other Internet-based services, platforms, and communications tools I use in my personal and professional capacities. A summary of those activities is included below.

Internet Service and Use

3. With the exception of a roughly two-year period described below, I have received Internet access at my home through various AT&T services from 1998 to today.

4. My initial Internet access through AT&T was via its Worldnet ("AT&T Worldnet") dial-up service, which I used until May 2005.

5. I later switched to using AT&T's High Speed Internet DSL ("AT&T DSL") service, using it from approximately May 2005 until 2016.

6. In 2016 I switched my service to a subscription from Charter Communications, which I used until April 2018.

7. In April 2018, I switched my Internet service back to AT&T.

8. I use the my Internet service through AT&T on a daily basis, and used my Charter Internet service similarly. I routinely use my Internet 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.

9. I use the Internet to send private messages and correspondence and to conduct other private activities online. I expect my Internet use, through the various AT&T and Charter services, for these private activities to remain private.

10. 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.

11. Some of these readers and listeners are in foreign countries. Throughout my time as a Charter, AT&T DSL, and AT&T 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.

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

Website Operations

13. I also operate and maintain several websites, many of which are associated with my blogging and podcast about urban homesteading. For example, I have operated websites such as www.rootsimple.com, www.homegrownevolution.org, and www.theurbanhomesteader.net since 2007 as part of these and other activities. I also have maintained www.urbanhomesteaderbook.com since 2007.

Email Communications

14. I use several email addresses, many of which are or were associated with my Internet subsciptions through AT&T. These are are hosted under the domain "sbcglobal.net," and the underlying service for these email addresses is provided by Yahoo! Inc.

15. I also use an email address provided by Google's gmail service, and have used it since December 2012.

16. I use my email as part of the activities described above, including sending private messages and corresponding with readers and listeners of my urban homesteading blog and podcast. I have always expected that these communications were private.

Additional Internet activities

17. I use social media services such as Facebook and Twitter for both personal reasons and related to my blogging and podcasting. I have had a Twitter account since 2009 and have multiple Facebook accounts that I began using in 2011.

18. I also rely on Internet communications services such as Skype for business purposes, while I use WhatsApp and WeChat to stay in touch with a friend living in China.

19. I also use Internet services such as Dropbox and Evernote to store files, keep notes, and help me stay organized and productive in both my work and home life.

Phone Services and Use

20. I receive residential phone service from AT&T, which, save for a roughly two-year period, I have used since 1998. AT&T's current phone service is provided as a Voice Over Internet Protocol, or VOIP, service.

21. Between 2016 and April 2018, I used Charter Communications for my residential phone service. Charter also provided a VOIP service.

22. Previously, I subscribed to residential phone service through AT&T from 1998 to 2016.

23. I also have used Google's Internet-based phone service, Google Voice, since 2015.

24. I have cellular phone service through a subscription to T-Mobile, which I first began using in 2015.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on September 26, 2018 at Los Angeles, California.

ERIK KNUTZEN

Plaintiff Erik Knutzen's
Communication and Internet Services

Type of service	Name of Provider/Service	Beginning date	End Date
Internet Service	AT&T	April 2018	Present
	Charter Communications	2016	April 2018
	AT&T	1998	2016
Residential Phone	AT&T	April 2018	Present
	Charter	2016	April 2018
	AT&T	1998	2016
	Google Voice	October 2010	Present
Cellular Phone	T-Mobile	2015	Present
Websites	www.rootsimple.com	September 2010	Present
	www.rootsimple.org	September 2010	Present
	www.homegrownevolution.com	December 2007	Present
	www.homegrownevolution.org	December 2007	Present
	www.survivela.com	January 2007	Present
	www.urbanhomesteaderbook.com	July 2007	Present
	www.theurbanhomesteader.net	July 2007	Present
	www.homegrownrevolution.org	July 2007	Present
	www.labreadbakers.com	March 2011	Present
	www.labreadbakers.org	March 2011	Present
Email	Accounts through sbcglobal.net	2000	2015
	Accounts through Google's Gmail	December 2012	Present
Social Media	Twitter	February 2009	Present
	Facebook (multiple accounts)	2011	Present
Other Online Services	WhatsApp	November 2016	Present
	Skype	September 2013	Present
	Dropbox	June 2017	Present
	Evernote	April 2010	Present

CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
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.: 4:08-cv-4373-JSW **DECLARATION OF JOICE WALTON IN OPPOSITION TO THE GOVERNMENT DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** September 28, 2018 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. Attached at the end of this declaration is a table describing the various Internet and phone services to which I have subscribed, along with a list of other Internet-based services, platforms, and communications tools I use in my personal and professional capacities. A summary of those activities is included below.

Internet Service and Use

3. I have received Internet service through AT&T since 2003. I currently receive Internet access at my home through a subscription to AT&T's U-Verse service. I have been a subscriber and user of this service since approximately March 2013.

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

5. After that, I was a subscriber and user of AT&T's High Speed Internet DSL ("AT&T DSL") service from February 2009 to March 2013.

6. I have used and continue to use the AT&T Internet services I have subscribed to 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.

7. I have relied on the AT&T U-Verse, 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.

8. 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.

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

Website Operations

10. I manage and operate several websites as part of my career as a recording artist and other professional endeavors.

11. For example, I currently operate www.joicewalton.com and have since June 2010. Vistitors to my website can hear my music, learn more about my work as a singer/songwriter, get information about upcoming performances, and purchase my music.

12. Previously, I operated www.pinnacle-records.com from 2014 to September 2018, which I used as part of my work as a recording artist. I also previously operated www.joicessong.com from October 2016 to February 2017.

13. I also currently operate www.browneyedgirlcoffee.com/ as part of the private label coffee company I founded and own. I've used the website since 2007.

Email Communications

14. I have several email addresses that I use for my professional and personal communications.

15. First, I have had multiple email addresses that are included as part of my AT&T Internet service. One was originally provided as part of my AT&T Worldnet subscription and it, along with others from AT&T, have been hosted under the domain "att.net." The underlying service for these email addresses is provided by Yahoo! Inc.

16. I also have had several email addresses associated with the various websites described above that I operate, the majority of which are hosted under the domains of those specific sites.

17. Additionally, I currently use a personal email address through Google's "gmail" email service that I have had since 2013.

18. 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 U-Verse, 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.

Additional Internet activities

19. I also use a number of other websites and Internet services, such as Facebook, Twitter, LinkedIn, Dropbox, and Google Drive, for both personal and professional pursuits.

Phone Services and Use

20. I currently receive residential phone service from Vonage, an Internet-based service that uses Voice Over IP, or VOIP, which I have subscribed to since 2013.

21. Previously, I was a subscriber and user of AT&T residential landline phone service from 2008 to 2013, and from 1995 to 2003.

22. Between those periods of AT&T service, I was a subscriber and user of Qwest Communications residential landline phone service from 2003 to 2008.

23. I currently receive cellular phone service from Verizon Wireless, and I have subscribed to the service since 2007.

24. Previously, I received cellular phone service from Cingular Wireless starting in 2005. When AT&T subsequently purchased Cingular, I continued to receive service from AT&T until 2007.

25. I have relied on both my residential and cellular phone services to send and receive phone calls of both a personal and professional nature. I have always expected that these communicaitons, and the fact that I made or received calls, to remain private.

26. I have also relied on my cellular phone service's data network to access the Internet and use phone-based applications, or apps, for a variety of purposes, such as messaging friends and co-workers, shopping, and banking.

27. Moreover, just as I rely on my residential Internet service for my career as a recording artist, I similarly rely on my cellular Internet service for the same reasons described above. This include promoting my music and interacting with fans.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on September 24, 2018 at San Jose, California.

JOICE WALTON

Plaintiff Joice Walton's
Communication and Internet Services

Type of service	Name of Provider/Service	Beginning date	End Date
Internet Service	AT&T U-Verse	March 2013	Present
	AT&T High-Speed Internet (DSL)	February 2009	March 2013
	AT&T World-Net dial-up Internet	At least March 2003	February 2009
Residential Phone	Vonage	2013	Present
	AT&T	2008	2013
	Qwest Communications	2003	2008
	AT&T	1995	2003
Cellular Phone	Verizon Wireless	2007	Present
	Cingular Wireless (later bought by AT&T)	2005	2007
Websites	www.joicewalton.com	2010	Present
	www.pinnacle-records.com	2014	Sept. 2018
	www.joicessong.com	October 2016	February 2017
	www.browneyedgirlcoffee.com	2007	Present
Email	Multiple accounts through AT&T	2000	Present
	Accounts through www.joicewalton.com	2010	Present
	Accounts through www.pinnacle-records.com	2014	Sept. 2018
	Accounts through www.joicessong.com	2016	February 2017
	Accounts through www.browneyedgirlcoffee.com	2008	Present
	Account through Google's Gmail	2013	Present
Social Media	Twitter	November 2016	Present
	Facebook	June 2013	Present
	LinkedIn	October 2013	Present
Other Online Services	Dropbox	August 2007	Present
	Google Drive	January 2013	Present

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 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.

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.

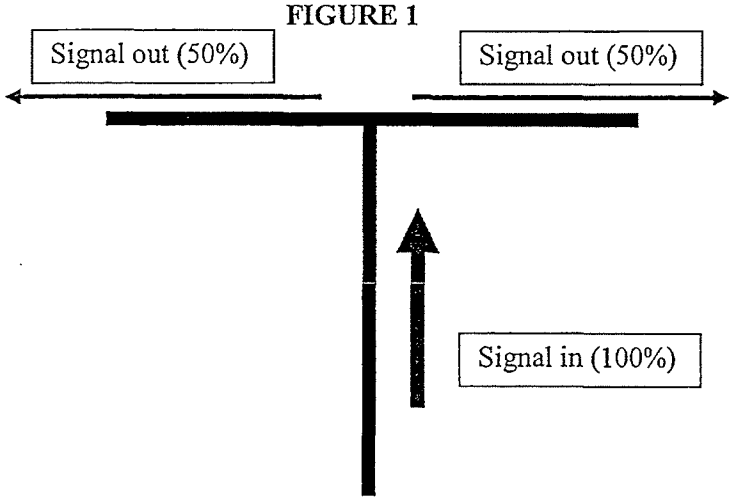
57. A splitter is a standard bit of optical gear. The simplest form is a "T" – one signal comes in, two signals go out. The splitters in this case were 50/50 splitters, which is to say that they split the signal such that 50% went to each output fiber. *See* the figure immediately below.

---

[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.

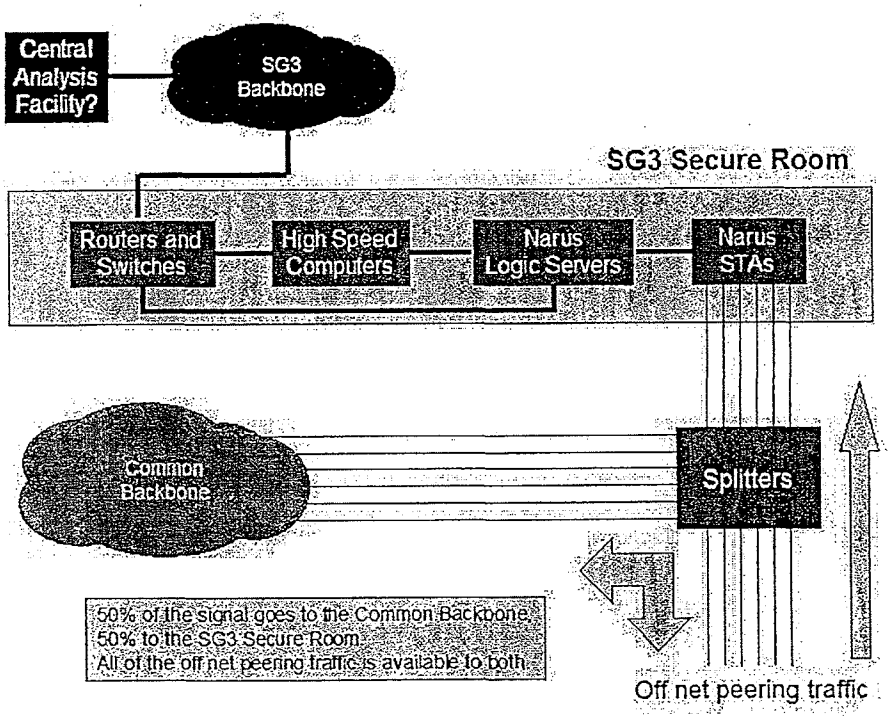
[28] I explained the function of a *splitter* earlier in this declaration, in the section on "Background – Fiber Optics". The T splitters used by AT&T apparently sent 50% of the input signal to each of two optic fiber cables, one of which conveyed the traffic to the SG3 Secure Room.

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.

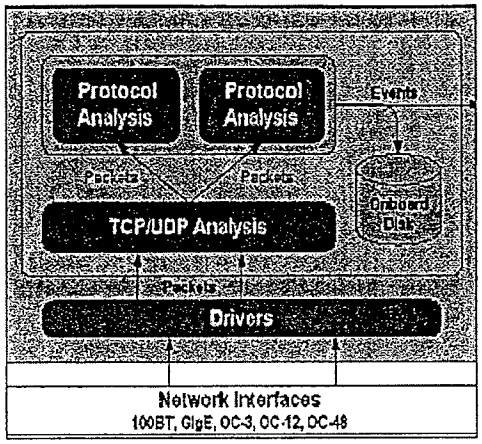
84. The following figure, which is taken from the Narus presentation to SCAMPI, makes it clear that the system, in addition to its other capabilities, is designed to identify traffic of interest and to act on it. It has the ability to store interesting traffic to the onboard disk that is part of the 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

---

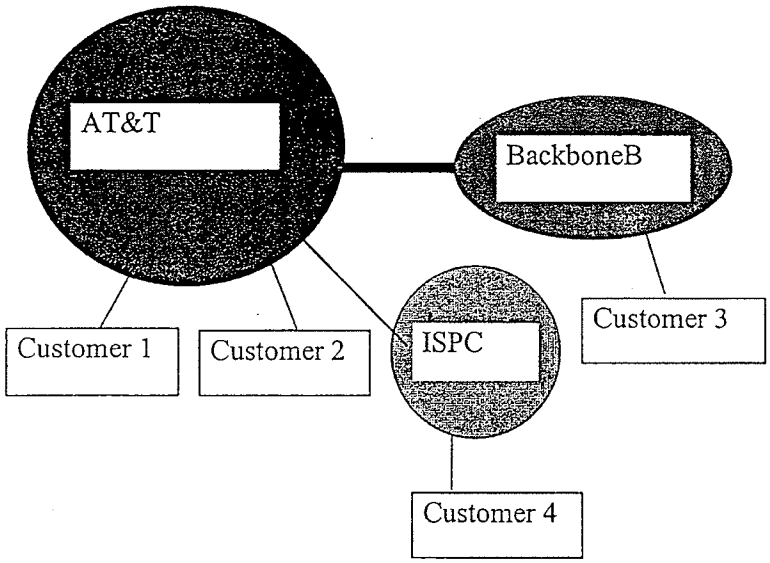
[39] See *In the Matter of AT&T Petition for Declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges,* FCC WC Docket 02-361, Petition of AT&T, at 24 (filed Oct. 18, 2002), at http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513386921 (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

KLEIN A-1

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:

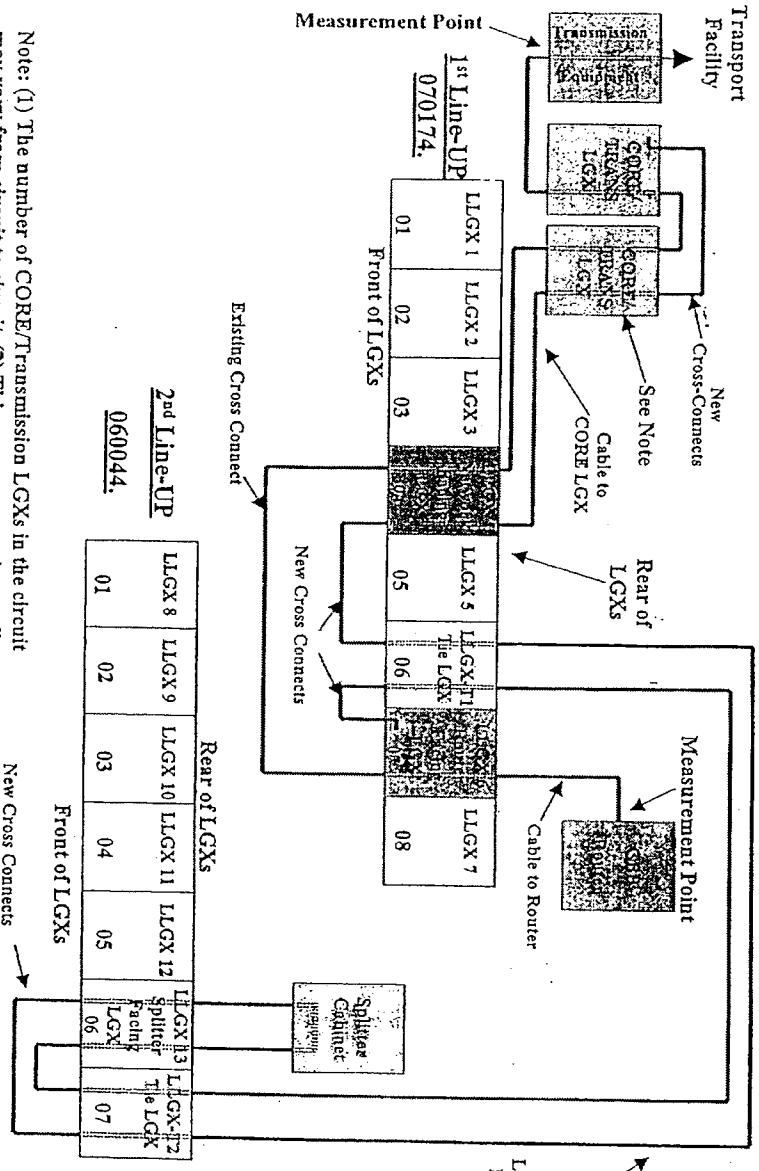
LGX Definition: There are multiple LGX bays affected by this procedure. Within the CBB LGX complex LGX bays follow a specific naming convention (LLGX 1, LLGX2, LLGX3, LLGX4, ...). This naming convention is uniform across sites. Since this document is designed to cover all sites, this uniform naming convention 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.

KLEIN B-6

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.502983	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.547606	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.502961	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.502960	3549		sffca01ck	POS 9/3		2/14/2003		2/18/2003	2/20/2003		
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.509438	1239		sffca02ck4	POS 11/0		2/21/2003		2/25/2003	2/27/2003		
14	Telia	OC-3	AGEC.671212	1299		sffca01ck	POS 0/1		2/21/2003		2/25/2003	2/27/2003		
15	PSINet	OC-3	AGEC.622380	174		sffca01ck	POS 0/2		2/21/2003		2/25/2003	2/27/2003		
16	Mae West	OC-3	AGEC.242541	nap		sffca82ck	POS 2/5		2/21/2003		2/25/2003	2/27/2003		

KLEIN B-20

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

KLEIN C-1

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,

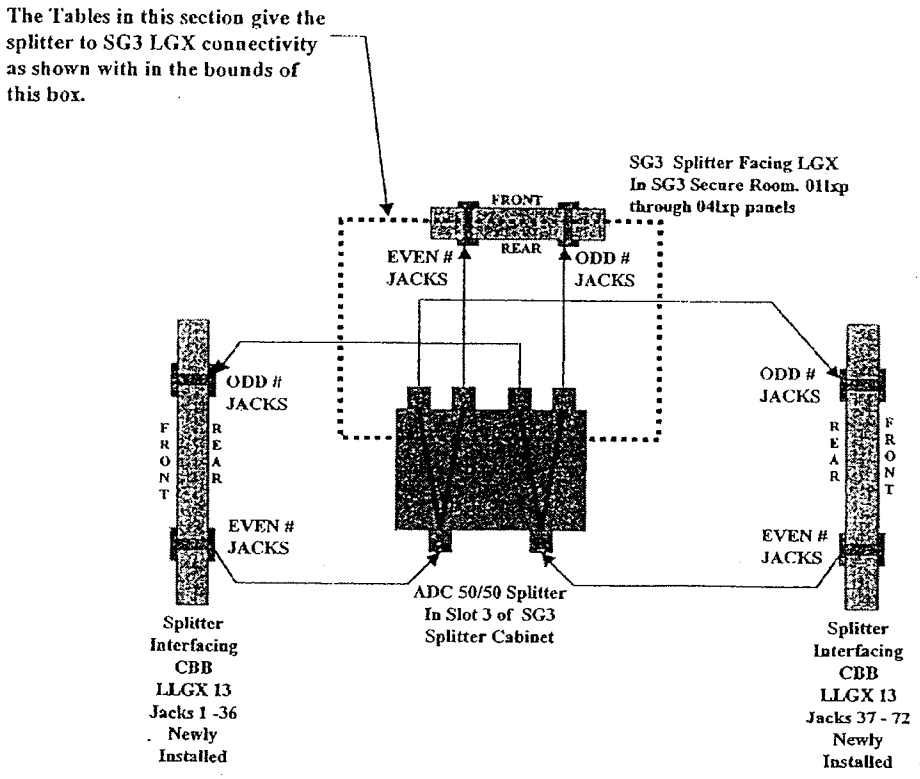
01lxp SG3 LGX Panel to Splitter Cabinet Connectivity

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

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



AT&T Proprietary

KLEIN C-46

Pages C-47 to C-58 redacted.