

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

U.S. FOREIGN  
INTELLIGENCE  
SURVEILLANCE COURT  
2014 MAR 11 PM 7:05

LEEANN FLYNN HALL  
CLERK OF COURT

---

IN RE APPLICATION OF THE  
FEDERAL BUREAU OF INVESTIGATION FOR  
AN ORDER REQUIRING THE PRODUCTION  
OF TANGIBLE THINGS

---

Docket Number: BR 14-01

**NOTICE OF ENTRY OF TEMPORARY RESTRAINING ORDER AGAINST THE  
UNITED STATES AND MOTION FOR TEMPORARY RELIEF FROM  
SUBPARAGRAPH (3)E OF PRIMARY ORDER**

The United States of America, hereby notifies this Court of the entry of a temporary restraining order (hereinafter, "TRO") yesterday, March 10, 2014, in two pending proceedings in the United States District Court for the Northern District of California: *Jewel, et al., v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), and *First Unitarian Church of Los Angeles, et al., v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.). The TRO prohibits, enjoins, and restrains various defendant government agencies, officials, and all those in active concert or participation with them from destroying any potential evidence relevant to the claims at issue in those civil actions, "including but not limited to prohibiting the destruction of any telephone metadata or 'call detail' records, pending further order" of that District Court. In light of the entry of this TRO, the United States respectfully moves this Court for temporary relief from the BR metadata destruction requirement set forth in subparagraph (3)E of the Primary Order entered in Docket Number BR 14-01, to allow the NSA to preserve

and retain BR metadata otherwise subject to destruction for non-analytic purposes under strict conditions set forth below pending resolution of the preservation issues raised by plaintiffs in *Jewel* and *First Unitarian Church* with the United States District Court for the Northern District of California.

1. Upon consideration of the Application by the United States, on January 3, 2014, the Honorable Thomas F. Hogan of this Court issued orders in the above-captioned docket number requiring the production to the NSA of certain BR metadata created by certain specified telecommunications providers. That authority expires on March 28, 2014, at 5:00 p.m. Eastern Time.<sup>1</sup> The application in docket number BR 14-01, including all exhibits and the resulting orders, as well as the Government's motion and the Court's February 5, 2014 Order, are incorporated herein by reference.

2. The Primary Order in the above-captioned docket number, as amended, requires NSA to strictly adhere to the enumerated minimization procedures, including subparagraph (3)E, which requires that "BR metadata be destroyed no later than five years (60 months) after its initial collection."

---

<sup>1</sup> On February 5, 2014, this Court also issued an order granting the Government's motion for amendment to the Primary Order to modify certain applicable minimization procedures. The minimization procedures were modified to require the Government, by motion, to first obtain the Court's approval to use specific selection terms to query the BR metadata for purposes of obtaining foreign intelligence information, except in cases of emergency, and to restrict queries of the BR metadata to return only that metadata within two "hops" of an approved seed.

3. On February 25, 2014, the Government moved this Court for a second amendment to the Primary Order in docket number BR 14-01, as amended, to allow the NSA to preserve and/or store the BR metadata for non-analytic purposes. As detailed in the Government's motion, several plaintiffs filed civil lawsuits<sup>2</sup> in several United States District Courts challenging, among other things, the legality of the Government's receipt of BR metadata from certain telecommunications service providers in response to production orders issued by this Court under Section 215. While the Court's Primary Order requires destruction of the BR metadata no later than five years (60 months) after its initial collection, the Government argued that such destruction could be inconsistent with its preservation obligations in connection with the pending civil litigation described

---

<sup>2</sup> Among the cases referenced in the Government's motion was *First Unitarian Church of Los Angeles, et al., v. National Security Agency, et al.*, No. C 13-03287 JSW (N.D. Cal.), one of the civil actions filed against various government agencies and officials challenging the legality of the NSA bulk telephony metadata collection program as authorized by the Court under Section 215. The Government's motion did not describe the pending civil action in *Jewel, et al., v. National Security Agency, et al.*, No. C 08-04373 JSW (N.D. Cal.) (hereinafter, "*Jewel*") and a companion case, *Shubert v. Obama*, No. C-07-0693-JSW (N.D. Cal.) (hereinafter, "*Shubert*"). Unlike the cases listed in the Government's Motion for Second Amendment to Primary Order, the claims raised in the *Jewel* and *Shubert* complaints challenge alleged intelligence activities conducted without court approval. In those cases, as the Government explained to plaintiffs' counsel, "the question of preservation of evidence ha[d] already been litigated in those cases" (on motions by the plaintiffs there) "and the court issued separate preservation orders that govern" in those actions. Those orders followed the Government's submission of a classified *ex parte* declaration that described in detail the specific preservation steps the government was taking. The orders direct the parties in *Jewel* and *Shubert*, *inter alia*, to halt "business practices" and "processes" that involve the destruction of "materials reasonably anticipated to be subject to discovery in th[ose] action[s]" "to the extent practicable for the pendency of [the] order[s]." Mot., Kurt Decl. Exh. A, at 3; *id.*, Exh. C at 3.

in the motion. Accordingly, to avoid the destruction of the BR metadata, the Government sought an amendment to the Court's Primary Order to allow the NSA under strict conditions to preserve and/or store the BR metadata for non-analytic purposes until relieved of its preservation obligations, or until further order of this Court. The Government's Motion for Second Amendment to Primary Order in docket number BR 14-01 is incorporated herein by reference.

4. By Opinion and Order dated March 7, 2014 this Court denied, without prejudice, the Government's motion. While the Court indicated that it was "reluctant to take any action that could impede the proper adjudication" of the lawsuits outlined in the Government's motion, and that it understood that the United States was proceeding with caution by seeking continued retention for preservation purposes, the Court ultimately concluded that it could not make the requisite findings to grant the motion based on the record before it. *Op.* at 12. The Court explained that "the proposed retention of the BR metadata beyond five years is unrelated to the government's need to obtain, produce, and disseminate foreign intelligence information" *Id.* at 7. It also noted that to date, no District Court or Circuit Court of Appeals had entered a preservation order in the cited litigation, none of the plaintiffs had sought discovery of the BR metadata, and none had made any effort to ensure its preservation. *Op.* at 8-9. As further described below, some of these circumstances have changed.

5. After the receipt of the Court's March 7, 2014 Opinion and Order, the Department of Justice assessed that prior to beginning destruction of the BR metadata, the Government should notify the plaintiffs and the District Courts in the relevant civil cases of the pending destruction. *See Op* at 11. Accordingly, on the same day, the Department began notifying the plaintiffs and district courts in the pending civil lawsuits listed in the Government's February 25, 2014 motion of this Court's Opinion and Order, and that consistent with the Order, as of the morning of Tuesday, March 11<sup>th</sup>, absent a contrary court order, the government would commence complying with the applicable destruction requirements. The Department also advised the NSA that unless a court instructed otherwise, destruction begin at the start of business on Tuesday, March 11, 2014.<sup>3</sup>

6. On March 10, 2014, plaintiffs in *Jewel* and *First Unitarian Church* moved in the United States District Court for the Northern District of California for TROs to prohibit destruction of the BR metadata, arguing that such data is evidence relevant to these lawsuits. True, correct and complete copies of the motions are attached hereto and incorporated by reference herein as Exhibits A and B. The District Court ordered the Government to file a response by 5:30 p.m. Eastern Time on March 10, and the Government filed a short response by that deadline.

---

<sup>3</sup> Following the entry of the TRO on March 10, 2014, the Department further advised NSA not to commence destruction as originally anticipated pending further court proceedings.

7. On March 10, 2014, the District Court entered an Order granting the temporary relief requested by plaintiffs. The District Court ordered that the Government defendants, "their officers, agents, servants[,] employees, and attorneys, and all those in active concert or participation with them are prohibited, enjoined, and restrained from destroying any potential evidence relevant to the claims at issue in this action, including but not limited to prohibiting the destruction of any telephone metadata or 'call detail' records, pending further order of the Court." The Court's TRO also set the following briefing/hearing schedule:

Plaintiffs' opening brief due March 13, 2013;

Government defendants' opposition brief due March 17, 2014;

Plaintiffs' reply brief due March 18, 2014; and

Hearing March 19, 2014.

A true, correct and complete copy of the order of the United States District Court for the Northern District of California is attached hereto as Exhibit C.

8. The United States is now subject to both (a) the order of this Court to destroy BR metadata no later than five years after its initial collection, and (b) the TRO entered by the United States District Court for the Northern District of California requiring that the BR metadata be retained and preserved pending resolution of the preservation issues raised by plaintiffs in *Jewel* and *First Unitarian Church*. In light of the developments in the district court litigation, and in order to complete the temporary restraining order

proceedings in the Northern District of California that would enable the development of additional facts or legal analysis relevant to topics discussed in this Court's March 7 Order, the Government respectfully requests that this Court grant temporary relief from the BR metadata destruction requirement set forth in subparagraph (3)E of the Primary Order entered in Docket Number BR 14-01 to allow the NSA to preserve and retain BR metadata otherwise subject to destruction solely for non-analytic purposes pending resolution of the preservation issues raised by plaintiffs in *Jewel* and *First Unitarian Church*, under the conditions described below.

9. Pending resolution of the preservation issues raised by plaintiffs in *Jewel* and *First Unitarian Church*, the Government proposes that all BR metadata retained beyond the five-year period specified in subparagraph (3)E of the Court's Primary Order will be preserved and/or stored in a format that precludes any access or use by NSA intelligence analysts for any purpose, including to conduct RAS-approved contact chaining queries of the BR metadata for the purpose of obtaining foreign intelligence information, and subject to the following additional conditions:

(i) NSA technical personnel may access BR metadata only for the purpose of ensuring continued compliance with the Government's preservation obligations to include taking reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued integrity of the BR metadata.

(ii) Should any further accesses to the BR metadata be required for civil litigation purposes, such accesses will occur only following prior written notice specifically describing the nature of and reason for the access, and the approval of this Court.

10. The Government will promptly notify this Court of any additional material developments in the district court litigation, including upon resolution of the TRO proceedings by the Northern District of California.

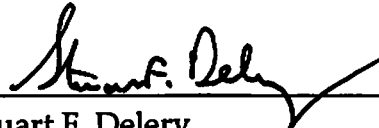


WHEREFORE, the United States of America, through the undersigned attorneys, respectfully moves for temporary relief from the BR metadata destruction requirement set forth in subparagraph (3)E of the Primary Order entered in Docket Number BR 14-01 to allow the NSA to preserve and retain BR metadata otherwise subject to destruction for non-analytic purposes as described above pending resolution of the preservation issues raised by plaintiffs in *Jewel* and *First Unitarian Church* with the United States District Court for the Northern District of California.

Respectfully submitted,



John P. Carlin  
Acting Assistant Attorney General  
National Security Division



Stuart F. Delery  
Assistant Attorney General  
Civil Division

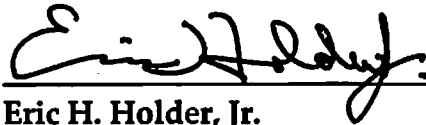
U.S. Department of Justice

**APPROVAL**

I hereby approve the filing of the foregoing Notice of Entry of Temporary Restraining Order Against the United States and Motion for Temporary Relief From Subparagraph (3)E of Primary Order with the United States Foreign Intelligence Surveillance Court.

March 11, 2014

Date



Eric H. Holder, Jr.

Attorney General of the United States

\_\_\_\_\_  
Date

\_\_\_\_\_  
James M. Cole

Deputy Attorney General of the United States

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

---

Docket Number: BR 14-01

**ORDER**

This matter having come before the Court upon the motion of the United States of America seeking temporary relief from the destruction requirement set forth in subparagraph (3)E of the Primary Order entered in Docket Number BR 14-01, which order requires the production to the National Security Agency (NSA) of certain call detail records or "telephony metadata" (hereinafter, "BR metadata") pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, and relying upon and incorporating the verified application, declaration, and all motions and orders issued in the above-captioned docket number, with full consideration having been given to the matters set forth therein, as well as the matters set forth in the Government's motion, and it appearing to the Court that the Government's motion for temporary relief should be granted,

IT IS HEREBY ORDERED that the Government's Motion for Temporary Relief from Subparagraph (3)E of Primary Order is GRANTED, and

IT IS FURTHER ORDERED the Government is authorized to preserve and retain BR metadata off-line beyond five years (60 months) after its initial collection pending resolution of the preservation issues raised by plaintiffs in *Jewel, et al., v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), and *First Unitarian Church of Los Angeles, et al., v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.), subject to the following conditions:

(i) all BR metadata retained beyond five-years (60 months) shall be preserved and/or stored in a format that precludes any access or use by NSA intelligence analysts for any purpose, including to conduct RAS-approved contact chaining queries of the BR metadata for the purpose of obtaining foreign intelligence information;

(ii) NSA technical personnel shall access BR metadata retained beyond five years (60 months) only for the purpose of ensuring continued compliance with the Government's preservation obligations to include taking reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued integrity of the BR metadata; and

(iii) should any further accesses to the BR metadata retained beyond five-years (60 months) be required for civil litigation purposes, such accesses shall occur only following prior written notice specifically describing the nature of and reason for the access, and the approval of this Court.

IT IS FURTHER ORDERED that all other provisions of the Court's Primary Order issued in docket number BR 14-01 shall remain in effect.

Signed \_\_\_\_\_ Eastern Time  
                    Date                      Time

\_\_\_\_\_  
**REGGIE B. WALTON**  
Presiding Judge, United States Foreign  
Intelligence Surveillance Court

1 CINDY COHN (SBN 145997)  
cindy@eff.org  
2 LEE TIEN (SBN 148216)  
KURT OPSAHL (SBN 191303)  
3 JAMES S. TYRE (SBN 083117)  
MARK RUMOLD (SBN 279060)  
4 ANDREW CROCKER (SBN 291596)  
ELECTRONIC FRONTIER FOUNDATION  
5 815 Eddy Street  
San Francisco, CA 94109  
6 Telephone: (415) 436-9333  
Fax: (415) 436-9993

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

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

THOMAS E. MOORE III (SBN 115107)  
tmoore@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

11  
12  
13  
14 *Counsel for Plaintiffs*

15  
16  
17 **UNITED STATES DISTRICT COURT**  
18 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
19 **SAN FRANCISCO DIVISION**

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

23 Plaintiffs,

24 v.

25 NATIONAL SECURITY AGENCY, *et al.*,

26 Defendants.

) CASE NO. 08-CV-4373-JSW

)  
)  
) **PLAINTIFFS' NOTICE OF EX PARTE**  
) **MOTION AND EX PARTE MOTION**  
) **FOR A TEMPORARY RESTRAINING**  
) **ORDER TO PREVENT THE**  
) **GOVERNMENT FROM DESTROYING**  
) **EVIDENCE**

) Date: March 10, 2014  
) Time: 1:30 p.m.  
) Courtroom 11, 19th Floor  
) The Honorable Jeffrey S. White

27 **IMMEDIATE RELIEF REQUESTED**  
28 **CRITICAL DATE: TUESDAY MORNING, MARCH 11, 2014**



1 this evidence is contrary to the Court's November 16, 2009 evidence preservation order (ECF  
2 No. 51) or otherwise contrary to the government defendants' discovery obligations.

3 The purpose of a TRO is to preserve the status quo and prevent irreparable harm "just so  
4 long as is necessary to hold a hearing, and no longer." *Granny Goose Foods, Inc. v. Brotherhood*  
5 *of Teamsters*, 415 U.S. 423, 439 (1974). This is exactly what is needed here.

6 There has been litigation challenging the lawfulness of the government's telephone  
7 metadata collection activity, Internet metadata collection activity, and upstream collection activity  
8 pending in the Northern District of California continuously since 2006. The government has been  
9 under evidence preservation orders in those lawsuits continuously since 2007.

10 The first-filed case was *Hepting v. AT&T*, No. 06-cv-0672 (N.D. Cal). It became the lead  
11 case in the MDL proceeding in this district, *In Re: National Security Agency Telecommunications*  
12 *Records Litigation*, MDL No. 06-cv-1791-VRW (N.D. Cal). On November 6, 2007, this Court  
13 entered an evidence preservation order in the MDL proceeding. ECF No. 393 in MDL No. 06-cv-  
14 1791-VRW. One of the MDL cases, *Virginia Shubert, et al., v. Barack Obama, et al.* No. 07-cv-  
15 0603-JSW (N.D. Cal.), remains in litigation today before this Court, and the MDL preservation  
16 order remains in effect today as to that case.

17 In 2008, movants filed this action—*Jewel v. NSA*—and this Court related it to the *Hepting*  
18 action. This Court entered an evidence preservation order in *Jewel*. ECF No. 51. The *Jewel*  
19 evidence preservation order remains in effect as of today.

20 The government has never sought to seek clarification of its preservation obligations  
21 regarding telephone metadata records from this Court or raised the issue with plaintiffs. Instead,  
22 the government defendants chose to raise the issue of preservation of telephone metadata records in  
23 an ex parte proceeding before the Foreign Intelligence Surveillance Court, without any notice to  
24 plaintiffs and without mentioning its obligations with regard to the same telephone records in *Jewel*  
25 *v. NSA* and *Shubert v. Obama*. Plaintiffs learned of the government's motion by reading the news  
26 media, and asked counsel for the government defendants to explain why they had not told the FISC  
27 about the *Jewel* evidence preservation order. See Cohn Decl, Exh. E.

28 Indeed, the government is aware and has acknowledged that destruction of the information



1 in question may conflict with the preservation orders issued in this and related cases: “While the  
2 Court’s Primary Order requires destruction of the BR metadata no longer than five years (60  
3 months) after its initial collection, such destruction could be inconsistent with the Government’s  
4 preservation obligations in connection with civil litigation pending against it. Accordingly, to  
5 avoid the destruction of the BR metadata, the Government seeks an amendment to the Court’s  
6 Primary Order that would allow the NSA to preserve and/or store the BR metadata for non-analytic  
7 purposes until relieved of its preservation obligations, or until further order of this Court under the  
8 conditions described below.” Government’s Motion for Second Amendment to Primary Order,  
9 FISC No. BR 14-01 (February 25, 2014). Although the government’s motion in the FISC did not  
10 discuss the preservation order in *Jewel*, this preservation order includes *the same* records at issue in  
11 *First Unitarian*.

#### 12 LEGAL STANDARD FOR TEMPORARY RESTRAINING ORDER

13 “A plaintiff seeking a [TRO] must establish that he is likely to succeed on the merits, that  
14 he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of  
15 equities tips in his favor, and that an injunction is in the public interest.” *Network Automation, Inc.*  
16 *v. Advanced Sys. Concepts*, 638 F.3d 1137, 1144 (9th Cir. 2011) (quoting *Winter v. Natural Res.*  
17 *Defense Council, Inc.*, 555 U.S. 7 (2008)).

#### 18 A. Likelihood of Success

19 The *Jewel* preservation order required the Government to “preserve evidence that may be  
20 relevant to this action.” The *Jewel* complaint alleged unlawful and unconstitutional acquisition of  
21 call-detail records, including the “call-detail records collected under the National Security Agency  
22 (NSA) bulk telephony metadata program” that the Government proposed to destroy.

23 Plaintiffs sought, among other relief, an injunction “requiring Defendants to provide to  
24 Plaintiffs and the class an inventory of their communications, records, or other information that  
25 was seized in violation of the Fourth Amendment.” Complaint, Prayer for Relief. This would be  
26 impossible if the records are destroyed. While the Plaintiff ultimately want the call-detail records  
27 destroyed at the conclusion of the case, there is no doubt the call-records “may be relevant” in the  
28 interim.

1 The Jewel order also required the Government to cease “destruction, recycling, relocation,  
2 or mutation of such materials.” Thus, the proposed destruction would be in direct violation of the  
3 Jewel preservation order.

4 **B. Irreparable Harm**

5 If the government proceeds with its planned destruction of evidence, the evidence will be  
6 gone. This is by definition irreparable.

7 **C. Balance of Equities**

8 While the Government contends it is required by the FISC to destroy the records  
9 immediately, the FISC order belies this assertion. The FISC denied the government's motion  
10 without prejudice to bringing another motion with additional facts and the FISC plainly was not  
11 informed of the preservation order in Jewel or even of its existence. The FISC clearly  
12 contemplated that the evidence destruction could wait while the government prepared and filed  
13 another motion, and continue until the Court considered and ruled on the motion.

14 **D. Public Interest**

15 These records are both an affront to the rights of millions of Americans and proof of their  
16 violation. Plaintiffs have no objection to severe restrictions on the Government's right to access  
17 and use the information, which will address the public interest in the documents being destroyed.  
18 However, it remains in the public interest to wait a short period of time before taking action, so that  
19 the fate of the documents can be addressed in an orderly fashion.

20 The necessity for this ex parte application could have been easily avoided had the  
21 government defendants followed the discovery and evidence preservation practices customary in  
22 this District. They could have, but did not, raised the issue of preserving telephone metadata  
23 records in the CMC statement meet-and-confer process in September 2013 (three months after the  
24 government defendants publicly acknowledged the phone records program), or at the Case  
25 Management Conference itself on September 27, 2013. They could have, but did not, raised this  
26 issue in the CMC statement meet-and-confer process in the related *First Unitarian* action during  
27 October 2013, or at the *First Unitarian* Case Management Conference itself on November 8, 2013.

28 Thereafter, at any point between November 8 and now the government defendants could

1 have raised the issue with plaintiffs by the meet-and-confer process, but they did not. They could  
2 have sought a further Case Management Conference before the Court or proceeded to raise the  
3 issue by noticed motion. Any of these manifold alternatives would have permitted the Court and  
4 the parties to address the issue in an orderly manner. By failing to pursue any of these alternatives,  
5 the government has made a temporary restraining order essential. Plaintiffs believe that no security  
6 is necessary under the circumstances. Plaintiffs respectfully request that the Court issue the order  
7 pending further proceedings on this issue.

8 DATE: March 10, 2014

Respectfully submitted,

9  
10 s/ Cindy Cohn  
CINDY COHN  
LEE TIEN  
11 KURT OPSAHL  
JAMES S. TYRE  
12 MARK RUMOLD  
ANDREW CROCKER  
13 ELECTRONIC FRONTIER FOUNDATION

14 RICHARD R. WIEBE  
LAW OFFICE OF RICHARD R. WIEBE

15 THOMAS E. MOORE III  
16 ROYSE LAW FIRM, PC

17 RACHAEL E. MENY  
PAULA L. BLIZZARD  
18 MICHAEL S. KWUN  
AUDREY WALTON-HADLOCK  
19 BENJAMIN W. BERKOWITZ  
20 KEKER & VAN NEST LLP

21 ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

22 *Counsel for Plaintiffs*

1 CINDY COHN (SBN 145997)  
cindy@eff.org  
2 LEE TIEN (SBN 148216)  
3 KURT OPSAHL (SBN 191303)  
4 JAMES S. TYRE (SBN 083117)  
MARK RUMOLD (SBN 279060)  
5 ANDREW CROCKER (SBN 291596)  
ELECTRONIC FRONTIER FOUNDATION  
6 815 Eddy Street  
San Francisco, CA 94109  
7 Telephone: (415) 436-9333  
Fax: (415) 436-9993

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

RACHAEL E. MENY (SBN 178514)  
rmeny@kvn.com  
PAULA L. BLIZZARD (SBN 207920)  
MICHAEL S. KWUN (SBN 198945)  
AUDREY WALTON-HADLOCK (SBN 250574)  
BENJAMIN W. BERKOWITZ (SBN 244441)  
KEKER & VAN NEST, LLP  
633 Battery Street  
San Francisco, 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

16 Attorneys for Plaintiffs

17 **UNITED STATES DISTRICT COURT**  
18 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
19 **SAN FRANCISCO DIVISION**

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

23 Plaintiffs,

24 v.

25 NATIONAL SECURITY AGENCY, *et al.*,

26 Defendants.  
27

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

) **DECLARATION OF CINDY COHN**

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

1 I, CINDY COHN, hereby declare:

2 1. I am a lawyer duly licensed to practice law in the State of California and before this  
3 district. I am the Legal Director of the Electronic Frontier Foundation, counsel of record for the  
4 plaintiffs.

5 2. I have attached to this Declaration true and correct copies of the following  
6 documents:

- 7 • **Exhibit A:** Complaint for Constitutional and Statutory Violations, Seeking  
8 Damages, Declaratory and Injunctive Relief in *Carolyn Jewel, et al., v. National*  
9 *Security Agency, et al.*, No. 08-cv-4373-JSW (N.D. Cal.) filed September 18, 2008;  
10 • **Exhibit B:** First Amended Complaint for Constitutional and Statutory  
11 Violations, Seeking Declaratory and Injunctive Relief in *First Unitarian Church of*  
12 *Los Angeles, et al. v. National Security Agency, et al.*, Case No. 13-cv-3287-JSW  
13 (N.D. Cal.) filed on March 7, 2014;  
14 • **Exhibit C:** Evidence Preservation Order in *Carolyn Jewel, et al., v. National*  
15 *Security Agency, et al.*, No. 08-cv-4373-JSW (N.D. Cal.) filed November 16, 2009;  
16 • **Exhibit D:** Evidence Preservation Order in *In Re: National Security Agency*  
17 *Telecommunications Records Litigation*, MDL No. 06-cv-1791-VRW (N.D. Cal.)  
18 dated November 6, 2007; and  
19 • **Exhibit E:** Emails between plaintiffs and defendants regarding preservation  
20 issues.

21 I declare under penalty of perjury under the laws of the United States that the foregoing is  
22 true and correct. Executed on March 10, 2014, at San Francisco, California.

23  
24 /s/ Cindy Cohn  
25 CINDY COHN  
26  
27  
28

# Exhibit A

# Exhibit A

1 ELECTRONIC FRONTIER FOUNDATION  
CINDY COHN (145997)  
2 cindy@eff.org  
LEE TIEN (148216)  
3 KURT OPSAHL (191303)  
KEVIN S. BANKSTON (217026)  
4 JAMES S. TYRE (083117)  
454 Shotwell Street  
5 San Francisco, CA 94110  
Telephone: 415/436-9333; Fax: 415/436-9993

6 RICHARD R. WIEBE (121156)  
7 wiebe@pacbell.net  
LAW OFFICE OF RICHARD R. WIEBE  
8 425 California Street, Suite 2025  
San Francisco, CA 94104  
9 Telephone: 415/433-3200; Fax: 415/433-6382

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

13 Attorneys for Plaintiffs

14 UNITED STATES DISTRICT COURT

15 NORTHERN DISTRICT OF CALIFORNIA

16 CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS,  
ERIK KNUTZEN and JOICE WALTON, on behalf of  
17 themselves and all others similarly situated,

18 Plaintiffs,

19 vs.

20 NATIONAL SECURITY AGENCY and KEITH B.  
ALEXANDER, its Director, in his official and personal  
21 capacities; MICHAEL V. HAYDEN, in his personal capacity;  
the UNITED STATES OF AMERICA; GEORGE W. BUSH,  
22 President of the United States, in his official and personal  
capacities; RICHARD B. CHENEY, in his personal capacity;  
23 DAVID S. ADDINGTON, in his personal capacity;  
DEPARTMENT OF JUSTICE and MICHAEL B.  
24 MUKASEY, its Attorney General, in his official and personal  
capacities; ALBERTO R. GONZALES, in his personal  
25 capacity; JOHN D. ASHCROFT, in his personal capacity;  
JOHN M. MCCONNELL, Director of National Intelligence, in  
26 his official and personal capacities; JOHN D. NEGROPONTE,  
in his personal capacity; and DOES #1-100, inclusive,

27 Defendants.  
28

ORIGINAL  
FILED

SEP 18 2008

RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

E-Filed

CASE NO:

CLASS ACTION

COMPLAINT FOR  
CONSTITUTIONAL AND  
STATUTORY  
VIOLATIONS, SEEKING  
DAMAGES,  
DECLARATORY, AND  
INJUNCTIVE RELIEF

CRB

DEMAND FOR JURY  
TRIAL





1           7.       In addition to eavesdropping on or reading specific communications, Defendants  
2 have indiscriminately intercepted the communications content and obtained the communications  
3 records of millions of ordinary Americans as part of the Program authorized by the President.

4           8.       The core component of the Program is Defendants' nationwide network of  
5 sophisticated communications surveillance devices, attached to the key facilities of  
6 telecommunications companies such as AT&T that carry Americans' Internet and telephone  
7 communications.

8           9.       Using this shadow network of surveillance devices, Defendants have acquired and  
9 continue to acquire the content of a significant portion of the phone calls, emails, instant messages,  
10 text messages, web communications and other communications, both international and domestic,  
11 of practically every American who uses the phone system or the Internet, including Plaintiffs and  
12 class members, in an unprecedented suspicionless general search through the nation's  
13 communications networks.

14           10.      In addition to using surveillance devices to acquire the domestic and international  
15 communications content of millions of ordinary Americans, Defendants have unlawfully solicited  
16 and obtained from telecommunications companies such as AT&T the complete and ongoing  
17 disclosure of the private telephone and Internet transactional records of those companies' millions  
18 of customers (including communications records pertaining to Plaintiffs and class members),  
19 communications records indicating who the customers communicated with, when and for how long,  
20 among other sensitive information.

21           11.      This non-content transactional information is analyzed by computers in conjunction  
22 with the vast quantity of communications content acquired by Defendants' network of surveillance  
23 devices, in order to select which communications are subjected to personal analysis by staff of the  
24 NSA and other Defendants, in what has been described as a vast "data-mining" operation.  
25  
26  
27  
28



1 claims on the NSA and the Department of Justice on December 19, 2007, and over six months have  
2 passed since the filing of that notice.

3 **PARTIES**

4 20. Plaintiff Tash Hepting, a senior systems architect, is an individual residing in  
5 Livermore, California. Hepting has been a subscriber and user of AT&T's residential long distance  
6 telephone service since at least June 2004.

7  
8 21. Plaintiff Gregory Hicks is an individual residing in San Jose, California. Hicks, a  
9 retired Naval Officer and systems engineer, has been a subscriber and user of AT&T's residential  
10 long distance telephone service since February 1995.

11 22. Plaintiff Carolyn Jewel is an individual residing in Petaluma, California. Jewel, a  
12 database administrator and author, has been a subscriber and user of AT&T's WorldNet dial-up  
13 Internet service since approximately June 2000.

14 23. Plaintiff Erik Knutzen is an individual residing in Los Angeles, California. Knutzen,  
15 a photographer and land use researcher, was a subscriber and user of AT&T's WorldNet dial-up  
16 Internet service from at least October 2003 until May 2005. Knutzen is currently a subscriber and  
17 user of AT&T's High Speed Internet DSL service.

18  
19 24. Plaintiff Joice Walton is an individual residing in San Jose, California. Walton, a  
20 high technology purchasing agent, is a current subscriber and user of AT&T's WorldNet dial-up  
21 Internet service. She has subscribed to and used this service since around April 2003.

22 25. Defendant National Security Agency (NSA) is an agency under the direction and  
23 control of the Department of Defense that collects, processes and disseminates foreign signals  
24 intelligence. It is responsible for carrying out the Program challenged herein.

25 26. Defendant Lieutenant General Keith B. Alexander is the current Director of the NSA,  
26 in office since April 2005. As NSA Director, defendant Alexander has ultimate authority for  
27 supervising and implementing all operations and functions of the NSA, including the Program.  
28

1           27.     Defendant Lieutenant General (Ret.) Michael V. Hayden is the former Director of  
2 the NSA, in office from March 1999 to April 2005. While Director, Defendant Hayden had ultimate  
3 authority for supervising and implementing all operations and functions of the NSA, including the  
4 Program.

5           28.     Defendant United States is the United States of America, its departments, agencies,  
6 and entities.

7           29.     Defendant George W. Bush is the current President of the United States, in office  
8 since January 2001. Mr. Bush authorized and continues to authorize the Program.

9           30.     Defendant Richard B. Cheney is the current Vice President of the United States, in  
10 office since January 2001. Defendant Cheney was personally involved in the creation, development  
11 and implementation of the Program.

12           31.     Defendant David S. Addington is currently the chief of staff to Defendant Cheney,  
13 in office since October 2005. Previously, Defendant Addington served as legal counsel to the Office  
14 of the Vice President. Defendant Addington was personally involved in the creation, development  
15 and implementation of the Program. On information and belief, Defendant Addington drafted the  
16 documents that purportedly authorized the Program.

17           32.     Defendant Department of Justice is a Cabinet-level executive department in the  
18 United States government charged with law enforcement, defending the interests of the United States  
19 according to the law, and ensuring fair and impartial administration of justice for all Americans.

20           33.     Defendant Michael B. Mukasey is the current Attorney General of the United States,  
21 in office since November 2007. As Attorney General, Defendant Mukasey approves and authorizes  
22 the Program on behalf of the Department of Justice.

23           34.     Defendant Alberto R. Gonzales is the former Attorney General of the United States,  
24 in office from February 2005 to September 2007, and also served as White House Counsel to  
25 President George W. Bush from January 2001 to February 2005. Defendant Gonzales was  
26 personally involved in the creation, development and implementation of the Program. As Attorney  
27

1 General, Defendant Gonzales authorized and approved the Program on behalf of the Department of  
2 Justice.

3 35. Defendant John D. Ashcroft is the former Attorney General of the United States, in  
4 office from January 2001 to February 2005. As Attorney General, Defendant Ashcroft authorized  
5 and approved the Program on behalf of the Department of Justice.  
6

7 36. Defendant Vice Admiral (Ret.) John M. McConnell is the Director of National  
8 Intelligence (“DNI”), in office since February 2007. Defendant McConnell has authority over the  
9 activities of the U.S. intelligence community, including the Program.

10 37. Defendant John D. Negroponte was the first Director of National Intelligence, in  
11 office from April 2005 to February 2007. As DNI, Defendant Negroponte had authority over the  
12 activities of the U.S. intelligence community, including the Program.

13 38. At all times relevant hereto, Defendants Doe Nos. 1-100, inclusive (the “Doe  
14 defendants”), whose actual names Plaintiffs have been unable to ascertain notwithstanding  
15 reasonable efforts to do so, but who are sued herein by the fictitious designation “Doe # 1” through  
16 “Doe # 100,” were agents or employees of the NSA, the DOJ, the White House, or were other  
17 government agencies or entities or the agents or employees of such agencies or entities, who  
18 authorized or participated in the Program. Plaintiffs will amend this complaint to allege their true  
19 names and capacities when ascertained. Upon information and belief each fictitiously named  
20 Defendant is responsible in some manner for the occurrences herein alleged and the injuries to  
21 Plaintiffs and class members herein alleged were proximately caused in relation to the conduct of  
22 Does 1-100 as well as the named Defendants.

23 **FACTUAL ALLEGATIONS RELATED TO ALL COUNTS**

24 **THE PRESIDENT’S AUTHORIZATION OF THE PROGRAM**

25 39. On October 4, 2001, President Bush, in concert with White House Counsel Gonzales,  
26 NSA Director Hayden, Attorney General Ashcroft and other Defendants, issued a secret presidential  
27 order (the “Program Order”) authorizing a range of surveillance activities inside of the United States  
28

1 without statutory authorization or court approval, including electronic surveillance of Americans'  
2 telephone and Internet communications (the "Program").

3 40. This Program of surveillance inside the United States began at least by October 6,  
4 2001, and continues to this day.

5 41. The President renewed and, on information and belief, renews his October 4, 2001  
6 order approximately every 45 days.

7 42. The Program of domestic surveillance authorized by the President and conducted by  
8 Defendants required and requires the assistance of major telecommunications companies such as  
9 AT&T, whose cooperation in the Program was and on information and belief is obtained based on  
10 periodic written requests from Defendants and/or other government agents indicating that the  
11 President has authorized the Program's activities, and/or based on oral requests from Defendants  
12 and/or other government agents.

13 43. The periodic written requests issued to colluding telecommunications companies,  
14 including AT&T, have stated and on information and belief do state that the Program's activities  
15 have been determined to be lawful by the Attorney General, except for one period of less than sixty  
16 days.

17 44. On information and belief, at some point prior to March 9, 2004, the Department of  
18 Justice concluded that certain aspects of the Program were in excess of the President's authority and  
19 in violation of criminal law.

20 45. On Tuesday, March 9, 2004, Acting Attorney General James Comey advised the  
21 Administration that he saw no legal basis for certain aspects of the Program. The then-current  
22 Program authorization was set to expire March 11, 2004.

23 46. On Thursday, March 11, 2004, the President renewed the Program Order without a  
24 certification from the Attorney General that the conduct it authorized was lawful.

25 47. On information and belief, the March 11 Program Order instead contained a  
26 statement that the Program's activities had been determined to be lawful by Counsel to the President  
27 Alberto Gonzales, and expressly claimed to override the Department of Justice's conclusion that the  
28

1 Program was unlawful as well as any act of Congress or judicial decision purporting to constrain the  
2 President's power as commander in chief.

3 48. For a period of less than sixty days, beginning on or around March 11, 2004, written  
4 requests to the telecommunications companies asking for cooperation in the Program stated that the  
5 Counsel to the President, rather than the Attorney General, had determined the Program's activities  
6 to be legal.

7 49. By their conduct in authorizing, supervising, and implementing the Program,  
8 Defendants, including the President, the Vice-President, the Attorneys General and the Directors of  
9 NSA since October 2001, the Directors of National Intelligence since 2005 and the Doe defendants,  
10 have aided, abetted, counseled, commanded, induced or procured the commission of all Program  
11 activities herein alleged, and proximately caused all injuries to Plaintiffs herein alleged.

12 **THE NSA'S DRAGNET INTERCEPTION OF COMMUNICATIONS TRANSMITTED**  
13 **THROUGH AT&T FACILITIES**

14 50. AT&T is a provider of electronic communications services, providing to the public  
15 the ability to send or receive wire or electronic communications.

16 51. AT&T is also a provider of remote computing services, providing to the public  
17 computer storage or processing services by means of an electronic communications system.

18 52. Plaintiffs and class members are, or at pertinent times were, subscribers to and/or  
19 customers of AT&T's electronic communications services and/or computer storage or processing  
20 services.

21 53. AT&T maintains domestic telecommunications facilities over which millions of  
22 Americans' telephone and Internet communications pass every day.

23 54. These facilities allow for the transmission of interstate and/or foreign electronic voice  
24 and data communications by the aid of wire, fiber optic cable, or other like connection between the  
25 point of origin and the point of reception.

26 55. One of these AT&T facilities is located at on Folsom Street in San Francisco, CA  
27 (the "Folsom Street Facility").

28

1           56.     The Folsom Street Facility contains a “4ESS Switch Room.” A 4ESS switch is a  
2 type of electronic switching system used to route long-distance telephone communications transiting  
3 through the facility.

4           57.     The Folsom Street Facility also contains a “WorldNet Internet Room” containing  
5 large routers, racks of modems for AT&T customers’ WorldNet dial-up services, and other  
6 telecommunications equipment through which wire and electronic communications to and from  
7 AT&T’s dial-up and DSL Internet service subscribers, including emails, instant messages, Voice-  
8 Over-Internet-Protocol (“VOIP”) conversations and web browsing requests, are transmitted.

9           58.     The communications transmitted through the WorldNet Internet room are carried as  
10 light signals on fiber-optic cables that are connected to routers for AT&T’s WorldNet Internet  
11 service and are a part of AT&T’s Common Backbone Internet network (“CBB”), which comprises  
12 a number of major hub facilities such as the Folsom Street Facility that are connected by a mesh of  
13 high-speed fiber optic cables and that are used for the transmission of interstate and foreign  
14 communications.

15           59.     The WorldNet Internet Room is designed to route and transmit vast amounts of  
16 Internet communications that are “peered” by AT&T between AT&T’s CBB and the networks of  
17 other carriers, such as ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global  
18 Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and MAE-West. “Peering” is the process  
19 whereby Internet providers interchange traffic destined for their respective customers, and for  
20 customers of their customers.

21           60.     Around January 2003, the NSA designed and implemented a program in  
22 collaboration with AT&T to build a surveillance operation at AT&T’s Folsom Street Facility, inside  
23 a secret room known as the “SG3 Secure Room”.

24           61.     The SG3 Secure Room was built adjacent to the Folsom Street Facility’s 4ESS  
25 switch room.

26           62.     An AT&T employee cleared and approved by the NSA was charged with setting up  
27 and maintaining the equipment in the SG3 Secure Room, and access to the room was likewise  
28 controlled by those NSA-approved AT&T employees.



1           63.     The SG3 Secure Room contains sophisticated computer equipment, including a  
2 device know as aNarus Semantic Traffic Analyzer (the Narus STA”), which is designed to analyze  
3 large volumes of communications at high speed, and can be programmed to analyze the contents and  
4 traffic patterns of communications according to user-defined rules.

5           64.     By early 2003, AT&T—under the instruction and supervision of the NSA—had  
6 connected the fiber-optic cables used to transmit electronic and wire communications through the  
7 WorldNet Internet Room to a “splitter cabinet” that intercepts a copy of all communications  
8 transmitted through the WorldNet Internet Room and diverts copies of those communications to the  
9 equipment in the SG3 Secure Room. (Hereafter, the technical means used to receive the diverted  
10 communications will be referred to as the “Surveillance Configuration.”)

11           65.     The equipment in the SG3 Secure Room is in turn connected to a private high-speed  
12 backbone network separate from the CBB (the “SG3 Network”).

13           66.     NSA analysts communicate instructions to the SG3 Secure Room’s equipment,  
14 including theNarus STA, using the SG3 Network, and the SG3 Secure Room’s equipment transmits  
15 communications based on those rules back to NSA personnel using the SG3 Network.

16           67.     The NSA in cooperation with AT&T has installed and is operating a nationwide  
17 network of Surveillance Configurations in AT&T facilities across the country, connected to the SG3  
18 Network.

19           68.     This network of Surveillance Configurations includes surveillance devices installed  
20 at AT&T facilities in Atlanta, GA; Bridgeton, MO; Los Angeles, CA; San Diego, CA; San Jose CA;  
21 and/or Seattle, WA.

22           69.     Those Surveillance Configurations divert all peered Internet traffic transiting those  
23 facilities into SG3 Secure Rooms connected to the secure SG3 Network used by the NSA, and  
24 information of interest is transmitted from the equipment in the SG3 Secure Rooms to the NSA  
25 based on rules programmed by the NSA.

26           70.     This network of Surveillance Configurations indiscriminately acquires domestic  
27 communications as well as international and foreign communications.

28

1           71.     This network of Surveillance Configurations involves considerably more locations  
2 than would be required to capture the majority of international traffic.

3           72.     This network of Surveillance Configurations acquires over half of AT&T's purely  
4 domestic Internet traffic, representing almost all of the AT&T traffic to and from other providers,  
5 and comprising approximately 10% of all purely domestic Internet communications in the United  
6 States, including those of non-AT&T customers.

7           73.     Through this network of Surveillance Configurations and/or by other means,  
8 Defendants have acquired and continue to acquire the contents of domestic and international wire  
9 and/or electronic communications sent and/or received by Plaintiffs and class members, as well as  
10 non-content dialing, routing, addressing and/or signaling information pertaining to those  
11 communications.

12           74.     In addition to acquiring all of the Internet communications passing through a number  
13 of key AT&T facilities, Defendants and AT&T acquire all or most long-distance domestic and  
14 international phone calls to or from AT&T long-distance customers, including both the content of  
15 those calls and dialing, routing, addressing and/or signaling information pertaining to those calls,  
16 by using a similarly nationwide network of surveillance devices attached to AT&T's long-distance  
17 telephone switching facilities, and/or by other means.

18           75.     The contents of communications to which Plaintiffs and class members were a party,  
19 and dialing, routing, addressing, and/or signaling information pertaining to those communications,  
20 were and are acquired by Defendants in cooperation with AT&T by using the nationwide network  
21 of Surveillance Configurations, and/or by other means.

22           76.     Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
23 class members' communications contents and non-content information is done without judicial,  
24 statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and  
25 in excess of statutory and constitutional authority.

26           77.     Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs'  
27 and class members' communications contents and non-content information is done without  
28

1 probable cause or reasonable suspicion to believe that Plaintiffs or class members have  
2 committed or are about to commit any crime or engage in any terrorist activity.

3 78. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
4 class members' communications contents and non-content information is done without probable  
5 cause or reasonable suspicion to believe that Plaintiffs or class members are foreign powers or agents  
6 thereof.

7 79. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
8 class members' communications contents and non-content information is done without any reason  
9 to believe that the information is relevant to an authorized criminal investigation or to an authorized  
10 investigation to protect against international terrorism or clandestine intelligence activities.

11 80. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
12 class members' communications contents and non-content information was directly performed,  
13 and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

14 81. On information and belief, Defendants will continue to directly acquire, and/or aid,  
15 abet, counsel, command, induce or procure the above-described acquisition in cooperation with  
16 AT&T, the communications contents and non-content information of Plaintiffs and class members.

17 **THE NSA'S DRAGNET COLLECTION OF COMMUNICATIONS RECORDS FROM**  
18 **AT&T DATABASES**

19 82. Defendants have since October 2001 continuously solicited and obtained the  
20 disclosure of all information in AT&T's major databases of stored telephone and Internet records,  
21 including up-to-the-minute updates to the databases that are disclosed in or near real-time.

22 83. Defendants have solicited and obtained from AT&T records concerning  
23 communications to which Plaintiffs and class members were a party, and continue to do so.

24 84. In particular, Defendants have solicited and obtained the disclosure of information  
25 managed by AT&T's "Daytona" database management technology, which includes records  
26 concerning both telephone and Internet communications, and continues to do so.  
27  
28

1           85.     Daytona is a database management technology designed to handle very large  
2 databases and is used to manage “Hawkeye,” AT&T’s call detail record (“CDR”) database, which  
3 contains records of nearly every telephone communication carried over its domestic network since  
4 approximately 2001, records that include the originating and terminating telephone numbers and the  
5 time and length for each call.

6           86.     The Hawkeye CDR database contains records or other information pertaining to  
7 Plaintiffs’ and class members’ use of AT&T’s long distance telephone service and dial-up Internet  
8 service.  
9

10          87.     As of September 2005, all of the CDR data managed by Daytona, when  
11 uncompressed, totaled more than 312 terabytes.

12          88.     Daytona is also used to manage AT&T’s huge network-security database, known as  
13 “Aurora,” which has been used to store Internet traffic data since approximately 2003. The Aurora  
14 database contains huge amounts of data acquired by firewalls, routers, honeypots and other devices  
15 on AT&T’s global IP (Internet Protocol) network and other networks connected to AT&T’s network.  
16

17          89.     The Aurora database managed by Daytona contains records or other information  
18 pertaining to Plaintiffs’ and class members’ use of AT&T’s Internet services.

19          90.     Since October 6, 2001 or shortly thereafter, Defendants have continually solicited  
20 and obtained from AT&T disclosure of the contents of the Hawkeye and Aurora communications  
21 records databases and/or other AT&T communications records, including records or other  
22 information pertaining to Plaintiffs’ and class members’ use of AT&T’s telephone and Internet  
23 services.

24          91.     The NSA and/or other Defendants maintain the communications records disclosed  
25 by AT&T in their own database or databases of such records.

26          92.     Defendants’ above-described solicitation of the disclosure by AT&T of Plaintiffs’  
27 and class members’ communications records, and its receipt of such disclosure, is done without  
28

1 judicial, statutory, or other lawful authorization, in violation of statutory and constitutional  
2 limitations, and in excess of statutory and constitutional authority.

3 93. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
4 and class members' communications records, and its receipt of such disclosure, is done without  
5 probable cause or reasonable suspicion to believe that Plaintiffs' or class members have  
6 committed or are about to commit any crime or engage in any terrorist activity.

7  
8 94. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
9 and class members' communications records, and its receipt of such disclosure, is done without  
10 probable cause or reasonable suspicion to believe that Plaintiffs' or class members are foreign  
11 powers or agents thereof.

12 95. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
13 and class members' communications records, and its receipt of such disclosure, is done without any  
14 reason to believe that the information is relevant to an authorized criminal investigation or to an  
15 authorized investigation to protect against international terrorism or clandestine intelligence  
16 activities.

17 96. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
18 and class members' communications records, and its receipt of such disclosure, is directly  
19 performed, and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

20 97. On information and belief, Defendants will continue to directly solicit and obtain  
21 AT&T's disclosure of its communications records, including records pertaining to Plaintiffs and  
22 class members, and/or will continue to aid, abet, counsel, command, induce or procure that conduct.

23 **CLASS ACTION ALLEGATIONS**

24 98. Pursuant to Federal Rules of Civil Procedure, Rule 23(b)(2), Plaintiffs Hepting,  
25 Hicks, Jewel, Knutzen, and Walton bring this action on behalf of themselves and a class of similarly  
26 situated persons defined as:  
27

28

1 All individuals in the United States that are current residential subscribers or  
2 customers of AT&T's telephone services or Internet services, or that were residential  
telephone or Internet subscribers or customers at any time after September 2001.

3 99. The class seeks certification of claims for declaratory, injunctive and other equitable  
4 relief pursuant to 18 U.S.C. §2520, 18 U.S.C. §2707 and 5 U.S.C. § 702, in addition to declaratory  
5 and injunctive relief for violations of the First and Fourth Amendments. Members of the class  
6 expressly and personally retain any and all damages claims they individually may possess arising  
7 out of or relating to the acts, events, and transactions that form the basis of this action. The  
8 individual damages claims of the class members are outside the scope of this class action.  
9

10 100. Excluded from the class are the individual Defendants, all who have acted in active  
11 concert and participation with the individual Defendants, and the legal representatives, heirs,  
12 successors, and assigns of the individual Defendants.

13 101. Also excluded from the class are any foreign powers, as defined by 50 U.S.C.  
14 § 1801(a), or any agents of foreign powers, as defined by 50 U.S.C. § 1801(b)(1)(A), including  
15 without limitation anyone who knowingly engages in sabotage or international terrorism, or  
16 activities that are in preparation therefore.  
17

18 102. This action is brought as a class action and may properly be so maintained pursuant  
19 to the provisions of the Federal Rules of Civil Procedure, Rule 23. Plaintiffs reserve the right to  
20 modify the class definition and the class period based on the results of discovery.

21 103. **Numerosity of the Class:** Members of the class are so numerous that their  
22 individual joinder is impracticable. The precise numbers and addresses of members of the class are  
23 unknown to the Plaintiffs. Plaintiffs estimate that the class consists of millions of members. The  
24 precise number of persons in the class and their identities and addresses may be ascertained from  
25 Defendants' and AT&T's records.  
26  
27  
28

1           104. **Existence of Common Questions of Fact and Law**: There is a well-defined  
2 community of interest in the questions of law and fact involved affecting the members of the class.

3 These common legal and factual questions include:

4           (a) Whether Defendants have violated the First and Fourth Amendment rights of  
5 class members, or are currently doing so;

6           (b) Whether Defendants have subjected class members to electronic surveillance,  
7 or have disclosed or used information obtained by electronic surveillance of the class members, in  
8 violation of 50 U.S.C. § 1809, or are currently doing so;

9           (c) Whether Defendants have intercepted, used or disclosed class members'  
10 communications in violation of 18 U.S.C. § 2511, or are currently doing so;

11           (d) Whether Defendants have solicited and obtained the disclosure of the  
12 contents of class members' communications in violation of 18 U.S.C. § 2703(a) or (b), or are  
13 currently doing so;

14           (e) Whether Defendants have solicited or obtained the disclosure of non-content  
15 records or other information pertaining to class members in violation of 18 U.S.C. § 2703(c), or are  
16 currently doing so;

17           (f) Whether Defendants have violated the Administrative Procedures Act, 5  
18 U.S.C. §§ 701 *et seq.*, or are currently doing so;

19           (g) Whether the Defendants have violated the constitutional principle of  
20 separation of powers, or are currently doing so;

21           (h) Whether Plaintiffs and class members are entitled to injunctive, declaratory,  
22 and other equitable relief against Defendants;

23           (i) Whether Plaintiffs and class members are entitled to an award of reasonable  
24 attorneys' fees and costs of this suit.

25           105. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the class  
26 because Plaintiffs are or were subscribers to the Internet and telephone services of Defendants.  
27  
28





1 of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of  
2 Plaintiffs' and class members' communications, contents of communications, and records pertaining  
3 to their communications transmitted, collected, and/or stored by AT&T, without judicial or other  
4 lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and  
5 constitutional limitations, and in excess of statutory and constitutional authority.  
6

7 111. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
8 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition,  
9 interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications,  
10 contents of communications, and records pertaining to their communications transmitted, collected,  
11 and/or stored by AT&T, without judicial or other lawful authorization, probable cause, and/or  
12 individualized suspicion.  
13

14 112. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the  
15 above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs and class  
16 members by obtaining judicial or other lawful authorization and by conforming their conduct to the  
17 requirements of the Fourth Amendment.  
18

19 113. By the acts alleged herein, Defendants have violated Plaintiffs' and class members'  
20 reasonable expectations of privacy and denied Plaintiffs and class members their right to be free  
21 from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution  
22 of the United States.  
23

24 114. By the acts alleged herein, Defendants' conduct has proximately caused harm to  
25 Plaintiffs and class members.  
26

27 115. Defendants' conduct was done intentionally, with deliberate indifference, or with  
28 reckless disregard of, Plaintiffs' and class members' constitutional rights.



1 of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of  
2 Plaintiffs' communications, contents of communications, and records pertaining to their  
3 communications transmitted, collected, and/or stored by AT&T without judicial or other lawful  
4 authorization, probable cause, and/or individualized suspicion, in violation of statutory and  
5 constitutional limitations, and in excess of statutory and constitutional authority.  
6

7 121. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
8 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition,  
9 interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of  
10 communications, and records pertaining to their communications transmitted, collected, and/or  
11 stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized  
12 suspicion.  
13

14 122. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the  
15 above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs by obtaining  
16 judicial or other lawful authorization and conforming their conduct to the requirements of the Fourth  
17 Amendment.  
18

19 123. By the acts alleged herein, Defendants have violated Plaintiffs' reasonable  
20 expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and  
21 seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.  
22

23 124. By the acts alleged herein, Defendants' conduct has proximately caused harm to  
24 Plaintiffs.  
25

26 125. Defendants' conduct was done intentionally, with deliberate indifference, or with  
27 reckless disregard of, Plaintiffs' constitutional rights.  
28

126. Plaintiffs seek an award of their actual damages and punitive damages against the  
Count II Defendants, and such other or further relief as is proper.

**COUNT III**

**Violation of First Amendment—Declaratory, Injunctive, and Other Equitable Relief**

**(Named Plaintiffs and Class vs. Defendants United States, National Security Agency, Department of Justice, Bush (in his official and personal capacities), Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)**

127. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

128. Plaintiffs and class members use AT&T's services to speak or receive speech anonymously and to associate privately.

129. Defendants directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications without judicial or other lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

130. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

131. By the acts alleged herein, Defendants violated Plaintiffs' and class members' rights to speak and to receive speech anonymously and associate privately under the First Amendment.





1           except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or  
2           any express statutory authorization that is an additional exclusive means for  
3           conducting electronic surveillance under section 1812 of this title; or (2)  
4           discloses or uses information obtained under color of law by electronic  
5           surveillance, knowing or having reason to know that the information was  
6           obtained through electronic surveillance not authorized by this chapter,  
7           chapter 119, 121, or 206 of Title 18 or any express statutory authorization  
8           that is an additional exclusive means for conducting electronic surveillance  
9           under section 1812 of this title.

10           145. In relevant part 50 U.S.C. § 1801 provides that:

11           (f) “Electronic surveillance” means – (1) the acquisition by an electronic,  
12           mechanical, or other surveillance device of the contents of any wire or radio  
13           communication sent by or intended to be received by a particular, known  
14           United States person who is in the United States, if the contents are acquired  
15           by intentionally targeting that United States person, under circumstances in  
16           which a person has a reasonable expectation of privacy and a warrant would  
17           be required for law enforcement purposes; (2) the acquisition by an  
18           electronic, mechanical, or other surveillance device of the contents of any  
19           wire communication to or from a person in the United States, without the  
20           consent of any party thereto, if such acquisition occurs in the United States,  
21           but does not include the acquisition of those communications of computer  
22           trespassers that would be permissible under section 2511(2)(i) of Title 18; (3)  
23           the intentional acquisition by an electronic, mechanical, or other surveillance  
24           device of the contents of any radio communication, under circumstances in  
25           which a person has a reasonable expectation of privacy and a warrant would  
26           be required for law enforcement purposes, and if both the sender and all  
27           intended recipients are located within the United States; or (4) the installation  
28           or use of an electronic, mechanical, or other surveillance device in the United  
          States for monitoring to acquire information, other than from a wire or radio  
          communication, under circumstances in which a person has a reasonable  
          expectation of privacy and a warrant would be required for law enforcement  
          purposes.

146. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this  
chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive*  
*means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act,  
and the interception of domestic wire, oral, and electronic communications may be conducted.”

(Emphasis added.)

147. 50 U.S.C. § 1812 further provides in relevant part that:

(a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
and 206 of Title 18 and this chapter shall be the *exclusive means* by which

1 electronic surveillance and the interception of domestic wire, oral, or  
2 electronic communications may be conducted.

3 (b) Only an express statutory authorization for electronic surveillance or the  
4 interception of domestic wire, oral, or electronic communications, other than  
as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
constitute an additional exclusive means for the purpose of subsection (a).

5 (Emphasis added.)

6 148. Defendants intentionally acquired, or aided, abetted, counseled, commanded,  
7 induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in,  
8 enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission  
9 of such acquisition, by means of a surveillance device, the contents of one or more wire  
10 communications to or from Plaintiffs and class members or other information in which Plaintiffs or  
11 class members have a reasonable expectation of privacy, without the consent of any party thereto,  
12 and such acquisition occurred in the United States.

14 149. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
15 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition  
16 of Plaintiffs' communications.

17 150. By the acts alleged herein, Defendants acting in excess of their statutory authority  
18 and in violation of statutory limitations have intentionally engaged in, or aided, abetted, counseled,  
19 commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused,  
20 participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in  
21 the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under color of law,  
22 not authorized by any statute, to which Plaintiffs and class members were subjected in violation of  
23 50 U.S.C. § 1809.

24 151. Additionally or in the alternative, by the acts alleged herein, Defendants acting in  
25 excess of their statutory authority and in violation of statutory limitations have intentionally  
26 disclosed or used information obtained under color of law by electronic surveillance, knowing or  
27  
28



1 having reason to know that the information was obtained through electronic surveillance not  
2 authorized by statute, including information pertaining to Plaintiffs and class members, or aided,  
3 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
4 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
5 or conspired in the commission of such acts.  
6

7 152. Defendants did not notify Plaintiffs or class members of the above-described  
8 electronic surveillance, disclosure, and/or use, nor did Plaintiffs or class members consent to such.

9 153. Plaintiffs and class members have been and are aggrieved by Defendants' electronic  
10 surveillance, disclosure, and/or use of their wire communications.

11 154. On information and belief, the Count V Defendants are now engaging in and will  
12 continue to engage in the above-described acts resulting in the electronic surveillance, disclosure,  
13 and/or use of Plaintiffs' and class members' wire communications, acting in excess of the Count V  
14 Defendants' statutory authority and in violation of statutory limitations, including 50 U.S.C. § 1809  
15 and 18 U.S.C. § 2511(2)(f), and are thereby irreparably harming Plaintiffs and class members.  
16 Plaintiffs and class members have no adequate remedy at law for the Count V Defendants'  
17 continuing unlawful conduct, and the Count V Defendants will continue to violate Plaintiffs' and  
18 class members' legal rights unless enjoined and restrained by this Court.  
19

20 155. Pursuant to *Larson v. United States*, 337 U.S. 682 (1949) and to 5 U.S.C. § 702,  
21 Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the  
22 class; enjoin the Count V Defendants, their agents, successors, and assigns, and all those in active  
23 concert and participation with them from violating the Plaintiffs' and class members' statutory  
24 rights, including their rights under 50 U.S.C. §§ 1801 *et seq.*; and award such other and further  
25 equitable relief as is proper.  
26  
27  
28

**COUNT VI**

**Violation of 50 U.S.C. § 1809, actionable under 50 U.S.C. § 1810—Damages**

**(Named Plaintiffs vs. Defendants United States, National Security Agency, Department of Justice, Alexander (in his official and personal capacities), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his official and personal capacities), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his official and personal capacities), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)**

156. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

157. In relevant part, 50 U.S.C. § 1809 provides that:

(a) Prohibited activities—A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

158. In relevant part 50 U.S.C. § 1801 provides that:

(f) “Electronic surveillance” means – (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio

1 communication, under circumstances in which a person has a reasonable  
2 expectation of privacy and a warrant would be required for law enforcement  
purposes.

3 159. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this  
4 chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive*  
5 *means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act,  
6 and the interception of domestic wire, oral, and electronic communications may be conducted.”  
7

8 (Emphasis added.)

9 160. 50 U.S.C. § 1812 further provides in relevant part that:

10 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
11 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
12 electronic surveillance and the interception of domestic wire, oral, or  
electronic communications may be conducted.

13 (b) Only an express statutory authorization for electronic surveillance or the  
14 interception of domestic wire, oral, or electronic communications, other than  
as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
constitute an additional exclusive means for the purpose of subsection (a).

15 (Emphasis added.)

16 161. Defendants intentionally acquired, or aided, abetted, counseled, commanded,  
17 induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in,  
18 enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission  
19 of such acquisition, by means of a surveillance device, the contents of one or more wire  
20 communications to or from Plaintiffs or other information in which Plaintiffs have a reasonable  
21 expectation of privacy, without the consent of any party thereto, and such acquisition occurred in  
22 the United States.  
23

24 162. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
25 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition  
26 of Plaintiffs’ communications.  
27  
28

1           163. By the acts alleged herein, Defendants have intentionally engaged in, or aided,  
2 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
3 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
4 or conspired in the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under  
5 color of law, not authorized by any statute, to which Plaintiffs were subjected in violation of 50  
6 U.S.C. § 1809.  
7

8           164. Additionally or in the alternative, by the acts alleged herein, Defendants have  
9 intentionally disclosed or used information obtained under color of law by electronic surveillance,  
10 knowing or having reason to know that the information was obtained through electronic surveillance  
11 not authorized by statute, including information pertaining to Plaintiffs, or aided, abetted, counseled,  
12 commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused,  
13 participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in  
14 the commission of such acts.  
15

16           165. Defendants did not notify Plaintiffs of the above-described electronic surveillance,  
17 disclosure, and/or use, nor did Plaintiffs consent to such.

18           166. Plaintiffs have been and are aggrieved by Defendants' electronic surveillance,  
19 disclosure, and/or use of their wire communications.  
20

21           167. Pursuant to 50 U.S.C. § 1810, which provides a civil action for any person who has  
22 been subjected to an electronic surveillance or about whom information obtained by electronic  
23 surveillance of such person has been disclosed or used in violation of 50 U.S.C. § 1809, Plaintiffs  
24 seek from the Court VI Defendants for each Plaintiff their statutory damages or actual damages;  
25 punitive damages as appropriate; and such other and further relief as is proper.  
26  
27  
28

**COUNT VII**

**Violation of 18 U.S.C. § 2511—Declaratory, Injunctive, and Other Equitable Relief**

**(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)**

168. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

169. In relevant part, 18 U.S.C. § 2511 provides that:

(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

170. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

171. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.”

(Emphasis added.)

172. 50 U.S.C. § 1812 further provides in relevant part that:

1 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
2 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
3 electronic surveillance and the interception of domestic wire, oral, or  
4 electronic communications may be conducted.

5 (b) Only an express statutory authorization for electronic surveillance or the  
6 interception of domestic wire, oral, or electronic communications, other than  
7 as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
8 constitute an additional exclusive means for the purpose of subsection (a).

9 (Emphasis added.)

10 173. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
11 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs'  
12 and class members' wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

13 174. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
14 endeavored to disclose, to another person the contents of Plaintiffs' and class members' wire or  
15 electronic communications, knowing or having reason to know that the information was obtained  
16 through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c);  
17 and/or

18 175. By the acts alleged herein, Defendants have intentionally and willfully used, or  
19 endeavored to use, the contents of Plaintiffs' and class members' wire or electronic communications,  
20 while knowing or having reason to know that the information was obtained through the interception  
21 of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(d).

22 176. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
23 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
24 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
25 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
26 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

27 177. Defendants have committed these acts of interception, disclosure, divulgence and/or  
28 use of Plaintiffs' and class members' communications directly or by aiding, abetting, counseling,

1 commanding, inducing, procuring, encouraging, promoting, instigating, advising, willfully causing  
2 participating in, enabling, contributing to, facilitating, directing, controlling, assisting in, or  
3 conspiring in their commission. In doing so, Defendants have acted in excess of their statutory  
4 authority and in violation of statutory limitations.

5  
6 178. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
7 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
8 divulgence and/or use of Plaintiffs' and class members' communications.

9 179. Defendants did not notify Plaintiffs or class members of the above-described  
10 intentional interception, disclosure, divulgence and/or use of their wire or electronic  
11 communications, nor did Plaintiffs or class members consent to such.

12 180. Plaintiffs and class members have been and are aggrieved by Defendants' intentional  
13 and willful interception, disclosure, divulgence and/or use of their wire or electronic  
14 communications.

15  
16 181. On information and belief, the Count VII Defendants are now engaging in and will  
17 continue to engage in the above-described acts resulting in the intentional and willful interception,  
18 disclosure, divulgence and/or use of Plaintiffs' and class members' wire or electronic  
19 communications, acting in excess of the Count VII Defendants' statutory authority and in violation  
20 of statutory limitations, including 18 U.S.C. § 2511, and are thereby irreparably harming Plaintiffs  
21 and class members. Plaintiffs and class members have no adequate remedy at law for the Count VII  
22 Defendants' continuing unlawful conduct, and the Count VII Defendants will continue to violate  
23 Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

24  
25 182. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose  
26 wire or electronic communications have been intercepted, disclosed, divulged or intentionally used  
27 in violation of 18 U.S.C. § 2511, to *Larson v. United States*, 337 U.S. 682 (1949), and to 5 U.S.C.  
28

1 § 702, Plaintiffs and class members seek equitable and declaratory relief against the Count VII  
2 Defendants.

3 183. Plaintiffs seek that this Court declare that Defendants have violated their rights and  
4 the rights of the class; enjoin the Count VII Defendants, their agents, successors, and assigns, and  
5 all those in active concert and participation with them from violating the Plaintiffs' and class  
6 members' statutory rights, including their rights under 18 U.S.C. § 2511; and award such other and  
7 further equitable relief as is proper.  
8

9 **COUNT VIII**

10 **Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2520—Damages**

11 **(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his**  
12 **personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity),**  
13 **Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his**  
14 **personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal**  
15 **capacity), and one or more of the Doe Defendants)**

16 184. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
17 paragraphs of this complaint, as if set forth fully herein.

18 185. In relevant part, 18 U.S.C. § 2511 provides that:

19 (1) Except as otherwise specifically provided in this chapter any person who  
20 – (a) intentionally intercepts, endeavors to intercept, or procures any other  
21 person to intercept or endeavor to intercept, any wire, oral, or electronic  
22 communication . . . (c) intentionally discloses, or endeavors to disclose, to  
23 any other person the contents of any wire, oral, or electronic communication,  
24 knowing or having reason to know that the information was obtained through  
25 the interception of a wire, oral, or electronic communication in violation of  
26 this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents  
27 of any wire, oral, or electronic communication, knowing or having reason to  
28 know that the information was obtained through the interception of a wire,  
oral, or electronic communication in violation of this subsection . . . shall be  
punished as provided in subsection (4) or shall be subject to suit as provided  
in subsection (5).

186. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or  
entity providing an electronic communication service to the public shall not  
intentionally divulge the contents of any communication (other than one to



1 such person or entity, or an agent thereof) while in transmission on that  
2 service to any person or entity other than an addressee or intended recipient  
of such communication or an agent of such addressee or intended recipient.

3 187. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this  
4 chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive*  
5 *means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act,  
6 and the interception of domestic wire, oral, and electronic communications may be conducted.”  
7

8 (Emphasis added.)

9 188. 50 U.S.C. § 1812 further provides in relevant part that:

10 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
11 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
12 electronic surveillance and the interception of domestic wire, oral, or  
electronic communications may be conducted.

13 (b) Only an express statutory authorization for electronic surveillance or the  
14 interception of domestic wire, oral, or electronic communications, other than  
as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
constitute an additional exclusive means for the purpose of subsection (a).

15 (Emphasis added.)

16 189. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
17 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs’  
18 wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or  
19

20 190. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
21 endeavored to disclose, to another person the contents of Plaintiffs’ wire or electronic  
22 communications, knowing or having reason to know that the information was obtained through the  
23 interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

24 191. By the acts alleged herein, Defendants have intentionally and willfully used, or  
25 endeavored to use, the contents of Plaintiffs’ wire or electronic communications, while knowing or  
26 having reason to know that the information was obtained through the interception of wire or  
27 electronic communications in violation of 18 U.S.C. § 2511(1)(d).  
28

1           192. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
2 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
3 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
4 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
5 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).  
6

7           193. Defendants have committed these acts of interception, disclosure, divulgence and/or  
8 use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing,  
9 procuring, encouraging, promoting, instigating, advising, willfully causing, participating in,  
10 enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their  
11 commission.  
12

13           194. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
14 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
15 divulgence and/or use of Plaintiffs' communications.  
16

17           195. Defendants did not notify Plaintiffs of the above-described intentional interception,  
18 disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or  
19 class members consent to such.  
20

21           196. Plaintiffs have been and are aggrieved by Defendants' intentional and willful  
22 interception, disclosure, divulgence and/or use of their wire or electronic communications.  
23

24           197. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose  
25 wire or electronic communications have been intercepted, disclosed, divulged or intentionally used  
26 in violation of 18 U.S.C. § 2511, Plaintiffs seek from the Court VIII Defendants for each Plaintiff  
27 their statutory damages or actual damages; punitive damages as appropriate; and such other and  
28 further relief as is proper.

**COUNT IX**

**Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2712—Damages Against The United States**

**(Named Plaintiffs vs. Defendants United States, Department of Justice, and National Security Agency)**

198. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

199. In relevant part, 18 U.S.C. § 2511 provides that:

(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

200. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

201. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.” (Emphasis added.)

202. 50 U.S.C. § 1812 further provides in relevant part that:

1 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
2 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
3 electronic surveillance and the interception of domestic wire, oral, or  
4 electronic communications may be conducted.

5 (b) Only an express statutory authorization for electronic surveillance or the  
6 interception of domestic wire, oral, or electronic communications, other than  
7 as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
8 constitute an additional exclusive means for the purpose of subsection (a).

9 (Emphasis added.)

10 203. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
11 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs'  
12 wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

13 204. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
14 endeavored to disclose, to another person the contents of Plaintiffs' wire or electronic  
15 communications, knowing or having reason to know that the information was obtained through the  
16 interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

17 205. By the acts alleged herein, Defendants have intentionally and willfully used, or  
18 endeavored to use, the contents of Plaintiffs' wire or electronic communications, while knowing or  
19 having reason to know that the information was obtained through the interception of wire or  
20 electronic communications in violation of 18 U.S.C. § 2511(1)(d).

21 206. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
22 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
23 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
24 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
25 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

26 207. Defendants have committed these acts of interception, disclosure, divulgence and/or  
27 use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing,  
28 procuring, encouraging, promoting, instigating, advising, willfully causing, participating in,

1 enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their  
2 commission.

3 208. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
4 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
5 divulgence and/or use of Plaintiffs' communications.  
6

7 209. Defendants did not notify Plaintiffs of the above-described intentional interception,  
8 disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or  
9 class members consent to such.

10 210. Plaintiffs have been and are aggrieved by Defendants' intentional and willful  
11 interception, disclosure, divulgence and/or use of their wire or electronic communications.  
12

13 211. Title 18 U.S.C. § 2712 provides a civil action against the United States and its  
14 agencies and departments for any person whose wire or electronic communications have been  
15 intercepted, disclosed, divulged or intentionally used in willful violation of 18 U.S.C. § 2511.  
16 Plaintiffs have complied fully with the claim presentment procedure of 18 U.S.C. § 2712. Pursuant  
17 to 18 U.S.C. § 2712, Plaintiffs seek from the Court IX Defendants for each Plaintiff their statutory  
18 damages or actual damages, and such other and further relief as is proper.  
19

20 **COUNT X**

21 **Violation of 18 U.S.C. § 2703(a) & (b)—Declaratory, Injunctive, and Other Equitable  
Relief**

22 **(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal  
23 capacities), Mukasey (in his official and personal capacities), and McConnell (in his official  
and personal capacities), and one or more of the Doe Defendants)**

24 212. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
25 paragraphs of this complaint, as if set forth fully herein.  
26

27 213. In relevant part, 18 U.S.C. § 2703 provides that:  
28

1 (a) Contents of Wire or Electronic Communications in Electronic Storage.— A  
2 governmental entity may require the disclosure by a provider of electronic  
3 communication service of the contents of a wire or electronic communication, that  
4 is in electronic storage in an electronic communications system for one hundred  
5 and eighty days or less, only pursuant to a warrant issued using the procedures  
6 described in the Federal Rules of Criminal Procedure by a court with jurisdiction  
7 over the offense under investigation or equivalent State warrant. A governmental  
8 entity may require the disclosure by a provider of electronic communications  
9 services of the contents of a wire or electronic communication that has been in  
10 electronic storage in an electronic communications system for more than one  
11 hundred and eighty days by the means available under subsection (b) of this  
12 section.

13 (b) Contents of Wire or Electronic Communications in a Remote Computing  
14 Service.—

15 (1) A governmental entity may require a provider of remote computing  
16 service to disclose the contents of any wire or electronic communication to  
17 which this paragraph is made applicable by paragraph (2) of this subsection—

18 (A) without required notice to the subscriber or customer, if the  
19 governmental entity obtains a warrant issued using the procedures  
20 described in the Federal Rules of Criminal Procedure by a court with  
21 jurisdiction over the offense under investigation or equivalent State  
22 warrant; or

23 (B) with prior notice from the governmental entity to the subscriber or  
24 customer if the governmental entity—

25 (i) uses an administrative subpoena authorized by a Federal or State  
26 statute or a Federal or State grand jury or trial subpoena; or

27 (ii) obtains a court order for such disclosure under subsection (d) of this  
28 section;

except that delayed notice may be given pursuant to section 2705 of this  
title.

(2) Paragraph (1) is applicable with respect to any wire or electronic  
communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from  
(or created by means of computer processing of communications received  
by means of electronic transmission from), a subscriber or customer of  
such remote computing service; and

(B) solely for the purpose of providing storage or computer processing  
services to such subscriber or customer, if the provider is not authorized to  
access the contents of any such communications for purposes of providing  
any services other than storage or computer processing.

214. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
or conspired in soliciting and obtaining from AT&T, the disclosure to Defendants of the contents

1 of Plaintiffs' and class members' communications while in electronic storage by an AT&T electronic  
2 communication service, and/or while carried or maintained by an AT&T remote computing service,  
3 in violation of 18 U.S.C. §§ 2703(a) and/or (b). In doing so, Defendants have acted in excess of  
4 their statutory authority and in violation of statutory limitations.

5  
6 215. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
7 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
8 and class members' communications.

9 216. Defendants did not notify Plaintiffs or class members of the disclosure of their  
10 communications, nor did Plaintiffs or class members consent to such.

11 217. Plaintiffs and class members have been and are aggrieved by Defendants' above-  
12 described soliciting and obtaining of disclosure of the contents of communications.

13  
14 218. On information and belief, the Count X Defendants are now engaging in and will  
15 continue to engage in the above-described soliciting and obtaining of disclosure of the contents of  
16 class members' communications while in electronic storage by AT&T's electronic communication  
17 service(s), and/or while carried or maintained by AT&T's remote computing service(s), acting in  
18 excess of the Count X Defendants' statutory authority and in violation of statutory limitations,  
19 including 18 U.S.C. § 2703(a) and (b), and are thereby irreparably harming Plaintiffs and class  
20 members. Plaintiffs and class members have no adequate remedy at law for the Count X  
21 Defendants' continuing unlawful conduct, and the Count X Defendants will continue to violate  
22 Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

23  
24 219. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved  
25 by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682  
26 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief  
27 against the Count X Defendants.  
28





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—  
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or  
(ii) obtains a court order for such disclosure under subsection (d) of this section;  
except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—  
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and  
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

223. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of the contents of Plaintiffs' communications while in electronic storage by an AT&T electronic communication service, and/or while carried or maintained by an AT&T remote computing service, in violation of 18 U.S.C. §§ 2703(a) and/or (b).

224. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' communications.

225. Defendants did not notify Plaintiffs of the disclosure of their communications, nor did Plaintiffs consent to such.

226. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and obtaining of disclosure of the contents of communications.



1 (ii) obtains a court order for such disclosure under subsection (d) of  
2 this section;  
3 except that delayed notice may be given pursuant to section 2705 of this  
4 title.

5 (2) Paragraph (1) is applicable with respect to any wire or electronic  
6 communication that is held or maintained on that service—  
7 (A) on behalf of, and received by means of electronic transmission from  
8 (or created by means of computer processing of communications received  
9 by means of electronic transmission from), a subscriber or customer of  
10 such remote computing service; and  
11 (B) solely for the purpose of providing storage or computer processing  
12 services to such subscriber or customer, if the provider is not authorized to  
13 access the contents of any such communications for purposes of providing  
14 any services other than storage or computer processing.

15 230. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
16 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
17 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
18 or conspired in the soliciting and obtaining from AT&T the disclosure to the NSA of the contents  
19 of Plaintiffs' communications while in electronic storage by an AT&T electronic communication  
20 service, and/or while carried or maintained by an AT&T remote computing service, in violation of  
21 18 U.S.C. §§ 2703(a) and/or (b).

22 231. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
23 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
24 communications.

25 232. Defendants did not notify Plaintiffs of the disclosure of their communications, nor  
26 did Plaintiffs consent to such.

27 233. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and  
28 obtaining of disclosure of the contents of communications.

29 234. Title 18 U.S.C. § 2712 provides a civil action against the United States and its  
30 agencies and departments for any person whose communications have been disclosed in willful

1 violation of 18 U.S.C. § 2703. Plaintiffs have complied fully with the claim presentment procedure  
2 of 18 U.S.C. § 2712. Pursuant to 18 U.S.C. § 2712, Plaintiffs seek from the Court XII Defendants  
3 for each Plaintiff their statutory damages or actual damages, and such other and further relief as is  
4 proper.

5  
6 **COUNT XIII**

7 **Violation of 18 U.S.C. § 2703(c)—Declaratory, Injunctive, and Other Equitable Relief**

8 **(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal**  
9 **capacities), Mukasey (in his official and personal capacities), and McConnell (in his official**  
10 **and personal capacities), and one or more of the Doe Defendants)**

11 235. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
12 paragraphs of this complaint, as if set forth fully herein.

13 236. In relevant part, 18 U.S.C. § 2703(c) provides that:

14 (c) Records Concerning Electronic Communication Service or Remote  
15 Computing Service.—

16 (1) A governmental entity may require a provider of electronic  
17 communication service or remote computing service to disclose a record or  
18 other information pertaining to a subscriber to or customer of such service  
19 (not including the contents of communications) only when the governmental  
20 entity—

21 (A) obtains a warrant issued using the procedures described in the Federal  
22 Rules of Criminal Procedure by a court with jurisdiction over the offense  
23 under investigation or equivalent State warrant;

24 (B) obtains a court order for such disclosure under subsection (d) of this  
25 section;

26 (C) has the consent of the subscriber or customer to such disclosure;

27 (D) submits a formal written request relevant to a law enforcement  
28 investigation concerning telemarketing fraud for the name, address, and  
place of business of a subscriber or customer of such provider, which  
subscriber or customer is engaged in telemarketing (as such term is  
defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing  
service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of  
session times and durations;

(D) length of service (including start date) and types of service utilized;

1 (E) telephone or instrument number or other subscriber number or  
2 identity, including any temporarily assigned network address; and  
3 (F) means and source of payment for such service (including any credit  
4 card or bank account number),

5 of a subscriber to or customer of such service when the governmental entity  
6 uses an administrative subpoena authorized by a Federal or State statute or a  
7 Federal or State grand jury or trial subpoena or any means available under  
8 paragraph (1).

9 (3) A governmental entity receiving records or information under this  
10 subsection is not required to provide notice to a subscriber or customer.

11 237. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
12 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
13 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
14 or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or  
15 other information pertaining to Plaintiffs' and class members' use of electronic communication  
16 services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C.  
17 § 2703(c). In doing so, Defendants have acted in excess of their statutory authority and in violation  
18 of statutory limitations.

19 238. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
20 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
21 and class members' records or other information.

22 239. Defendants did not notify Plaintiffs or class members of the disclosure of these  
23 records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs  
24 or class members consent to such.

25 240. Plaintiffs and class members have been and are aggrieved by Defendants' above-  
26 described acts of soliciting and obtaining disclosure by AT&T of records or other information  
27 pertaining to Plaintiffs and class members.

28 241. On information and belief, the Court XIII Defendants are now engaging in and will  
continue to engage in the above-described soliciting and obtaining disclosure by AT&T of records  
or other information pertaining to Plaintiffs and class members, acting in excess of the Court XIII

1 Defendants' statutory authority and in violation of statutory limitations, including 18 U.S.C. §  
2 2703(c), and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class  
3 members have no adequate remedy at law for the Count XIII Defendants' continuing unlawful  
4 conduct, and the Count XIII Defendants will continue to violate Plaintiffs' and class members' legal  
5 rights unless enjoined and restrained by this Court.  
6

7 242. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved  
8 by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682  
9 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief  
10 against the Count XIII Defendants.

11 243. Plaintiffs seek that the Court declare that Defendants have violated their rights and  
12 the rights of the class; enjoin the Count XIII Defendants, their agents, successors, and assigns, and  
13 all those in active concert and participation with them from violating the Plaintiffs' and class  
14 members' statutory rights, including their rights under 18 U.S.C. § 2703; and award such other and  
15 further equitable relief as is proper.  
16

#### 17 COUNT XIV

#### 18 **Violation of 18 U.S.C. § 2703(c), actionable under 18 U.S.C. § 2707—Damages**

19 **(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his**  
20 **personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity),**  
21 **Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his**  
22 **personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal**  
23 **capacity), and one or more of the Doe Defendants)**

24 244. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
25 paragraphs of this complaint, as if set forth fully herein.

26 245. In relevant part, 18 U.S.C. § 2703(c) provides that:

27 (c) Records Concerning Electronic Communication Service or Remote  
28 Computing Service.—

(1) A governmental entity may require a provider of electronic  
communication service or remote computing service to disclose a record or

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

246. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- (C) has the consent of the subscriber or customer to such disclosure;
  - (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
  - (E) seeks information under paragraph (2).
- (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
- (A) name;
  - (B) address;
  - (C) local and long distance telephone connection records, or records of session times and durations;
  - (D) length of service (including start date) and types of service utilized;
  - (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
  - (F) means and source of payment for such service (including any credit card or bank account number),
- of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
- (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

253. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).

254. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' records or other information.

255. Defendants did not notify Plaintiffs of the disclosure of these records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs consent to such.





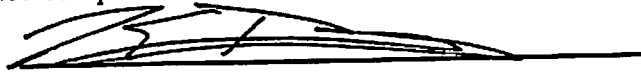


**JURY DEMAND**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: September 17, 2008



ELECTRONIC FRONTIER FOUNDATION  
CINDY COHN (1455997)  
LEE TIEN (148216)  
KURT OPSAHL (191303)  
KEVIN S. BANKSTON (217026)  
JAMES S. TYRE (083117)  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: 415/436-9333  
415/436-9993 (fax)

RICHARD R. WIEBE (121156)  
LAW OFFICE OF RICHARD R. WIEBE  
425 California Street, Suite 2025  
San Francisco, CA 94104  
Telephone: (415) 433-3200  
Facsimile: (415) 433-6382

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

Attorneys for Plaintiffs

# Exhibit B

# Exhibit B

1 CINDY COHN (SBN 145997)  
 cindy@eff.org  
 2 LEE TIEN (SBN 148216)  
 KURT OPSAHL (SBN 191303)  
 3 MATTHEW ZIMMERMAN (SBN 212423)  
 MARK RUMOLD (SBN 279060)  
 4 DAVID GREENE (SBN 160107)  
 JAMES S. TYRE (SBN 083117)  
 5 ELECTRONIC FRONTIER FOUNDATION  
 815 Eddy Street  
 6 San Francisco, CA 94109  
 Tel.: (415) 436-9333; Fax: (415) 436-9993  
 7  
 THOMAS E. MOORE III (SBN 115107)  
 8 tmoore@moorelawteam.com  
 ROYSE LAW FIRM, PC  
 9 1717 Embarcadero Road  
 Palo Alto, CA 94303  
 10 Tel.: 650-813-9700; Fax: 650-813-9777  
 11 Attorneys for Plaintiffs

RACHAEL E. MENY (SBN 178514)  
 rmeny@kvn.com  
 MICHAEL S. KWUN (SBN 198945)  
 BENJAMIN W. BERKOWITZ (SBN 244441)  
 KEKER & VAN NEST, LLP  
 633 Battery Street  
 San Francisco, California 94111  
 Tel.: (415) 391-5400; Fax: (415) 397-7188  
 RICHARD R. WIEBE (SBN 121156)  
 wiebe@pacbell.net  
 LAW OFFICE OF RICHARD R. WIEBE  
 One California Street, Suite 900  
 San Francisco, CA 94111  
 Tel.: (415) 433-3200; Fax: (415) 433-6382  
 ARAM ANTARAMIAN (SBN 239070)  
 aram@eff.org  
 LAW OFFICE OF ARAM ANTARAMIAN  
 1714 Blake Street  
 Berkeley, CA 94703  
 Telephone: (510) 289-1626

12  
 13 **UNITED STATES DISTRICT COURT**  
 14 **NORTHERN DISTRICT OF CALIFORNIA**  
 15 **SAN FRANCISCO DIVISION**

16 FIRST UNITARIAN CHURCH OF LOS )  
 ANGELES; ACORN ACTIVE MEDIA; BILL OF )  
 17 RIGHTS DEFENSE COMMITTEE; CALGUNS )  
 FOUNDATION, INC.; CALIFORNIA )  
 ASSOCIATION OF FEDERAL FIREARMS )  
 18 LICENSEES, INC.; CHARITY AND SECURITY )  
 NETWORK; COUNCIL ON AMERICAN )  
 19 ISLAMIC RELATIONS-CALIFORNIA; )  
 COUNCIL ON AMERICAN ISLAMIC )  
 20 RELATIONS-OHIO; COUNCIL ON )  
 AMERICAN ISLAMIC RELATIONS- )  
 21 FOUNDATION, INC.; FRANKLIN ARMORY; )  
 FREE PRESS; FREE SOFTWARE )  
 22 FOUNDATION; GREENPEACE, INC.; HUMAN )  
 RIGHTS WATCH; MEDIA ALLIANCE; )  
 23 NATIONAL LAWYERS GUILD; NATIONAL )  
 ORGANIZATION FOR THE REFORM OF )  
 24 MARIJUANA LAWS, CALIFORNIA CHAPTER;) )  
 PATIENT PRIVACY RIGHTS; PEOPLE FOR )  
 25 THE AMERICAN WAY; PUBLIC )  
 KNOWLEDGE; SHALOM CENTER; )  
 26 STUDENTS FOR SENSIBLE DRUG POLICY; )  
 TECHFREEDOM; and UNITARIAN )  
 27 UNIVERSALIST SERVICE COMMITTEE, )  
 28 **Plaintiffs.** )

Case No: 3:13-cv-03287 JSW

**FIRST AMENDED COMPLAINT  
 FOR CONSTITUTIONAL AND  
 STATUTORY VIOLATIONS,  
 SEEKING DECLARATORY AND  
 INJUNCTIVE RELIEF**

Hon. Jeffrey S. White  
 Courtroom 11 - 19th Floor

**DEMAND FOR JURY TRIAL**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

v.

NATIONAL SECURITY AGENCY and KEITH  
B. ALEXANDER, its Director, in his official and  
individual capacities; the UNITED STATES OF  
AMERICA; DEPARTMENT OF JUSTICE and  
ERIC H. HOLDER, its Attorney General, in his  
official and individual capacities; Acting Assistant  
Attorney General for National Security JOHN P.  
CARLIN, in his official and individual capacities;  
FEDERAL BUREAU OF INVESTIGATION and  
JAMES B. COMEY, its Director, in his official  
and individual capacities; ROBERT S.  
MUELLER, former Director of the FEDERAL  
BUREAU OF INVESTIGATION, in his individual  
capacity; JAMES R. CLAPPER, Director of  
National Intelligence, in his official and individual  
capacities, and DOES 1-100,

Defendants.











1           19. Plaintiff Bill of Rights Defense Committee (BORDC) is a non-profit, advocacy  
2 organization based in Northhampton, Massachusetts. BORDC supports an ideologically, politically,  
3 ethnically, geographically, and generationally diverse grassroots movement focused on educating  
4 Americans about the erosion of fundamental freedoms; increasing civic participation; and converting  
5 concern and outrage into political action. BORDC brings this action on behalf of itself and its  
6 adversely affected staff.

7           20. Plaintiff Calguns Foundation, Inc. (CGF) is a non-profit, membership organization  
8 based in San Carlos, California. CGF works to support the California firearms community by  
9 promoting education for all stakeholders about California and federal firearm laws, rights, and  
10 privileges, and defending and protecting the civil rights of California gun owners. In particular, CGF  
11 operates a hotline for those with legal questions about gun rights in California. Plaintiff CGF brings  
12 this action on behalf of itself and on behalf of its adversely affected members and staff.

13           21. Plaintiff California Association of Federal Firearms Licensees, Inc. (CAL-FFL) is a  
14 non-profit, industry association of, by, and for firearms manufacturers, dealers, collectors, training  
15 professionals, shooting ranges, and others, advancing the interests of its members and the general  
16 public through strategic litigation, legislative efforts, and education. CAL-FFL expends financial and  
17 other resources in both litigation and non-litigation projects to protect the interests of its members  
18 and the public at large. CAL-FFL brings this action on behalf of itself and its adversely affected  
19 members and staff.

20           22. Plaintiff Charity and Security Network's mission is to protect civil society's ability to  
21 carry out peacebuilding projects, humanitarian aid, and development work effectively and in a  
22 manner consistent with human rights principles and democratic values. To accomplish this, the  
23 Network focuses on: coordinating advocacy by bringing together stakeholders from across the  
24 nonprofit sector with policymakers to support needed changes in U.S. national security rules; and  
25 raising awareness, dispelling myths and promoting awareness of the positive contribution civil  
26 society makes to human security. CSN brings this action on behalf of itself and its adversely affected  
27 membership and staff.

28

1           23.    Plaintiffs Council on American Islamic Relations – California (CAIR-CA), Council on  
2 American Islamic Relations-Ohio (CAIR-OHIO), and Council on American Islamic Relations-  
3 Foundation, Inc. (CAIR-F) are non-profit, advocacy organization with offices in California, Ohio,  
4 and Washington, D.C., respectively. CAIR-CA, CAIR-OHIO, and CAIR-F’s missions are to  
5 enhance the understanding of Islam, encourage dialogue, protect civil liberties, empower American  
6 Muslims, and build coalitions that promote justice and mutual understanding. CAIR-CA, CAIR-  
7 OHIO, and CAIR-F bring this action on behalf of themselves and their adversely affected staffs.

8           24.    Plaintiff Franklin Armory, a wholly owned subsidiary of CBE, Inc., is a state and  
9 federally licensed manufacturer of firearms located in Morgan Hill, California. Franklin Armory  
10 specializes in engineering and building products for restrictive firearms markets, such as California.  
11 Franklin Armory is a member of CAL-FFL. Franklin Armory brings this suit on its own behalf.

12           25.    Plaintiff Free Press is a non-profit, advocacy organization based in Washington, D.C.  
13 Free Press’s mission is to build a nationwide movement to change media and technology policies,  
14 promote the public interest, and strengthen democracy by advocating for universal and affordable  
15 Internet access, diverse media ownership, vibrant public media, and quality journalism. Free Press  
16 brings this action on behalf of itself and its adversely affected members and staff.

17           26.    Plaintiff the Free Software Foundation (FSF) is a non-profit, membership organization  
18 based in Boston, Massachusetts. FSF helped pioneer a worldwide free software movement and  
19 provides an umbrella of legal and technical infrastructure for collaborative software development  
20 internationally. FSF brings this action on behalf of itself and its adversely affected members and  
21 staff.

22           27.    Plaintiff Greenpeace, Inc. (Greenpeace) is a non-profit, membership organization  
23 headquartered in Washington, D.C. Through a domestic and international network of offices and  
24 staff, Greenpeace uses research, advocacy, public education, lobbying, and litigation to expose  
25 global environmental problems and to promote solutions that are essential to a green and peaceful  
26 future. Greenpeace brings this action on behalf of itself and its adversely affected members and staff.

27           28.    Plaintiff Human Rights Watch (HRW) is a non-profit, advocacy organization, based in  
28

1 New York, New York. Through its domestic and international network of offices and staff, HRW  
2 challenges governments and those in power to end abusive practices and respect international human  
3 rights law by enlisting the public and the international community to support the cause of human  
4 rights for all. HRW brings this action on behalf of itself and its adversely affected staff.

5 29. Plaintiff Media Alliance is a non-profit, membership organization based in Oakland,  
6 California. Media Alliance serves as a resource and advocacy center for media workers, non-profit  
7 organizations, and social justice activists to make media accessible, accountable, decentralized,  
8 representative of society's diversity, and free from covert or overt government control and corporate  
9 dominance. Media Alliance brings this action on behalf of itself and its adversely affected members  
10 and staff.

11 30. Plaintiff National Lawyers Guild, Inc. is a non-profit corporation formed in 1937 as  
12 the nation's first racially integrated voluntary bar association. For over seven decades the Guild has  
13 represented thousands of Americans critical of government policies, from antiwar, environmental  
14 and animal rights activists, to Occupy Wall Street protesters, to individuals accused of computer-  
15 related offenses. From 1940-1975 the FBI conducted a campaign of surveillance, investigation and  
16 disruption against the Guild and its members, trying unsuccessfully to label it a subversive  
17 organization. The NLG brings this action on behalf of itself and its adversely affected membership  
18 and staff.

19 31. Plaintiff National Organization for the Reform of Marijuana Laws, California Chapter  
20 (NORML, California Chapter) is a non-profit, membership organization located in Berkeley,  
21 California. NORML, California Chapter is dedicated to reforming California's marijuana laws and  
22 its mission is to establish the right of adults to use cannabis legally. NORML, California Chapter  
23 brings this action on behalf of itself and its adversely affected members and staff.

24 32. Plaintiff Patient Privacy Rights (PPR) is a bipartisan, non-profit organization with  
25 12,000 members in all 50 states. It works to give patients control over their own sensitive health  
26 information in electronic systems, with the goal of empowering privacy and choices that protect jobs  
27 and opportunities and ensure trust in the patient-physician relationship. The lack of privacy of health  
28

1 information causes millions of individuals every year to refuse or delay needed medical treatment or  
2 hide information, putting their health at risk. PPR brings this action on behalf of itself and its  
3 adversely affected members and volunteers.

4 33. Plaintiff People for the American Way (PFAW) is a non-profit, membership  
5 organization based in Washington, D.C. With over 595,000 members, PFAW's primary function is  
6 the education of its members, supporters, and the general public as to important issues that impact  
7 fundamental civil and constitutional rights and freedoms, including issues concerning civil liberties,  
8 government secrecy, improper government censorship, and First Amendment freedoms. PFAW  
9 brings this action on behalf of itself and its adversely affected members and staff.

10 34. Plaintiff Public Knowledge is a non-profit, advocacy organization based in  
11 Washington, D.C. Public Knowledge is dedicated to preserving the openness of the Internet and the  
12 public's access to knowledge, promoting creativity through the balanced application of copyright  
13 laws, and upholding and protecting the rights of consumers to use innovative technology lawfully.  
14 Public Knowledge brings this action on behalf of itself and its adversely affected staff.

15 35. Plaintiff the Shalom Center seeks to be a prophetic voice in Jewish, multireligious, and  
16 American life. It connects the experience and wisdom of the generations forged in the social,  
17 political, and spiritual upheavals of the last half-century with the emerging generation of activists,  
18 addressing with special concern the planetary climate crisis and the power configurations behind that  
19 crisis. The Shalom Center brings this action on behalf of itself and its adversely affected membership  
20 and staff.

21 36. Plaintiff Students for Sensible Drug Policy (SSDP) is a non-profit, membership  
22 organization based in Washington, D.C. With over 3,000 members, SSDP is an international,  
23 grassroots network of students who are concerned about the impact drug abuse has on our  
24 communities, but who also know that the War on Drugs is failing our generation and our society.  
25 SSDP creates change by bringing young people together and creating safe spaces for students of all  
26 political and ideological stripes to have honest conversations about drugs and drug policy. SSDP  
27 brings this action on behalf of itself and its adversely affected membership and staff.



1           37. Plaintiff TechFreedom is a non-profit, think tank based in Washington, D.C.  
2 TechFreedom's mission is promoting technology that improves the human condition and expands  
3 individual capacity to choose by educating the public, policymakers, and thought leaders about the  
4 kinds of public policies that enable technology to flourish. TechFreedom seeks to advance public  
5 policy that makes experimentation, entrepreneurship, and investment possible, and thus unleashes  
6 the ultimate resource: human ingenuity. TechFreedom brings this action on behalf of itself and its  
7 adversely affected staff.

8           38. Plaintiff Unitarian Universalist Service Committee (UUSC) is a non-profit,  
9 membership organization based in Cambridge, Massachusetts. UUSC advances human rights and  
10 social justice around the world, partnering with those who confront unjust power structures and  
11 mobilizing to challenge oppressive policies. Through a combination of advocacy, education, and  
12 partnerships with grassroots organizations, UUSC promotes economic rights, advances  
13 environmental justice, defends civil liberties, and preserves the rights of people in times of  
14 humanitarian crisis. UUSC brings this action on behalf of itself and its adversely affected members  
15 and staff.

16           39. All Plaintiffs make and receive telephone calls originating within the United States in  
17 furtherance of their mission and operations. In particular, Plaintiffs make and receive telephone calls  
18 to and from their members, staffs, and constituents, among other groups and individuals seeking to  
19 associate with them, in furtherance of their mission and operations, including advancing their  
20 political beliefs, exchanging ideas, and formulating strategy and messages in support of their causes.

21           40. Each of the Plaintiffs above is a membership organization and brings this action on  
22 behalf of its members has members whose communications information has been collected as part of  
23 the Associational Tracking Program.

24           41. Defendant NSA is an agency under the direction and control of the Department of  
25 Defense that seizes, collects, processes, and disseminates signals intelligence. It is responsible for  
26 carrying out at least some of the Associational Tracking Program challenged herein.

27           42. Defendant General Keith B. Alexander is the current Director of the NSA, in office  
28

1 since April of 2005. As NSA Director, General Alexander has authority for supervising and  
2 implementing all operations and functions of the NSA, including the Associational Tracking  
3 Program. General Alexander personally authorizes and supervises the Associational Tracking  
4 Program.

5 43. Defendant United States is the United States of America, its departments, agencies,  
6 and entities.

7 44. Defendant Department of Justice is a Cabinet-level executive department in the United  
8 States government charged with law enforcement, defending the interests of the United States  
9 according to the law, and ensuring fair and impartial administration of justice for all Americans.

10 45. Defendant Eric H. Holder is the current Attorney General of the United States, in  
11 office since February of 2009. Attorney General Holder personally approves, authorizes, supervises,  
12 and participates in the Associational Tracking Program on behalf of the Department of Justice.

13 46. Defendant John B. Carlin is the current Acting Assistant Attorney General for  
14 National Security. In that position, defendant Carlin participates in the Department of Justice's  
15 implementation of the Associational Tracking Program.

16 47. Defendant Federal Bureau of Investigation (FBI) is a component of the Department of  
17 Justice that conducts federal criminal investigation and collects domestic intelligence. FBI is  
18 responsible for carrying out at least some of the Associational Tracking Program activities  
19 challenged herein.

20 48. Defendant James B. Comey is the current Director of the FBI, in office since  
21 September of 2013. As FBI Director, defendant Comey has ultimate authority for supervising and  
22 implementing all operations and functions of the FBI, including its participation in the Associational  
23 Tracking Program. Defendant Comey personally authorizes and supervises the FBI's participation in  
24 the Associational Tracking Program.

25 49. Defendant Robert S. Mueller is the previous Director of the FBI, from September,  
26 2001-September, 2013. As FBI Director, defendant Mueller had ultimate authority for supervising  
27 and implementing all operations and functions of the FBI, including its participation in the  
28

1 Associational Tracking Program. Defendant Mueller personally authorized and supervised the FBI's  
2 participation in the Associational Tracking Program.

3 50. Defendant Lieutenant General (Ret.) James R. Clapper is the Director of National  
4 Intelligence (DNI), in office since August of 2010. Defendant Clapper participates in the activities of  
5 the U.S. intelligence community, including the Associational Tracking Program.

6 51. Defendants DOES 1-100 are persons or entities who have authorized or participated in  
7 the Associational Tracking Program. Plaintiffs will allege their true names and capacities when  
8 ascertained. Upon information and belief each is responsible in some manner for the occurrences  
9 herein alleged and the injuries to Plaintiffs herein alleged were proximately caused by the acts or  
10 omissions of DOES 1-100 as well as the named Defendants.

11 **FACTUAL ALLEGATIONS RELATED TO ALL COUNTS**

12 **STATUTORY BACKGROUND**

13 52. 50 U.S.C § 1861, the codification of section 215 of the USA PATRIOT Act, as  
14 amended, is entitled "Access to certain business records for foreign intelligence and surveillance  
15 purposes." Section 1861 provides narrow and limited authority for the Foreign Intelligence  
16 Surveillance Court (FISC) to issue orders for the production of "any tangible things (including  
17 books, records, papers, documents, and other items) for an investigation to obtain foreign  
18 intelligence information not concerning a United States person or to protect against international  
19 terrorism or clandestine intelligence activities." The limitations on section 1861 orders include the  
20 following:

- 21
- 22 • an order may be issued only upon "a statement of facts showing that there are  
23 reasonable grounds to believe that the tangible things sought are relevant to an  
24 authorized investigation;"
  - 25 • the tangible things sought to be produced by an order must be described "with  
26 sufficient particularity to permit them to be fairly identified;" and
  - 27 • an order "may only require the production of a tangible thing if such thing can be  
28 obtained with a *subpoena duces tecum* issued by a court of the United States in aid of

1 a grand jury investigation or with any other order issued by a court of the United  
2 States directing the production of records or tangible things.”

3 **THE ASSOCIATIONAL TRACKING PROGRAM**

4 53. The Associational Tracking Program is electronic surveillance that collects and  
5 acquires telephone communications information for all telephone calls transiting the networks of all  
6 major American telecommunication companies, including Verizon, AT&T, and Sprint. Every day,  
7 the Associational Tracking Program collects information about millions of telephone calls made by  
8 millions of Americans. This includes information about all calls made wholly within the United  
9 States, including local telephone calls, as well as communications between the United States and  
10 abroad.

11 54. Defendants’ Associational Tracking Program collects and acquires call detail records  
12 and comprehensive communications routing information about telephone calls. The collected  
13 information includes, but is not limited to, session identifying information (*e.g.*, originating and  
14 terminating telephone number, International Mobile Subscriber Identity (IMSI) number,  
15 International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone  
16 calling card numbers, and time and duration of call. Defendants acquire this information through the  
17 use of a surveillance device.

18 55. Beginning in 2001, participating phone companies voluntarily provided telephone  
19 communications information for the Associational Tracking program to Defendants. Since 2006, the  
20 FISC, at the request of Defendants, has issued orders under 50 U.S.C. § 1861 purporting to compel  
21 the production of communications information, including communications information not yet in  
22 existence, on an ongoing basis, as part of the Associational Tracking Program.

23 56. As an example, attached hereto as Exhibit A, and incorporated herein by this  
24 reference, is an Order issued under 50 U.S.C. § 1861 requiring the production of communications  
25 information for use in the Associational Tracking Program.

26 57. DNI Clapper has admitted the Order is authentic, as indicated in Exhibit B, attached  
27 hereto and incorporated by this reference.

28

1           58.     The Order is addressed to Verizon Business Network Services Inc., on behalf of MCI  
2 Communications Services Inc., d/b/a Verizon Business Services (individually and collectively  
3 “Verizon”). Verizon is one of the largest providers of telecommunications services in the United  
4 States with over 98 million subscribers. Through its subsidiaries and other affiliated entities that it  
5 owns, controls, or provides services to, Verizon provides telecommunications services to the public  
6 and to other entities. These subsidiaries and affiliated entities include Verizon Business Global,  
7 LLC; MCI Communications Corporation; Verizon Business Network Services, Inc.; MCI  
8 Communications Services, Inc.; and Verizon Wireless (Cellco Partnership).

9                           **BULK SEIZURE COLLECTION, ACQUISITION, AND STORAGE**

10           59.     The Associational Tracking Program seizes, collects and acquires telephone  
11 communications information for all telephone calls transiting the networks of all major American  
12 telecommunication companies, including Verizon, AT&T, and Sprint.

13           60.     The telephone communications information Defendants seize, collect and acquire in  
14 bulk as part of the Associational Tracking Program is retained and stored by Defendants in one or  
15 more databases. These databases contain call information for all, or the vast majority, of calls wholly  
16 within the United States, including local telephone calls, and calls between the United States and  
17 abroad, for a period of at least five years. Defendants have indiscriminately obtained and stored the  
18 telephone communications information of millions of ordinary Americans, including Plaintiffs, their  
19 members, and staffs, as part of the Associational Tracking Program.

20           61.     Defendants’ bulk seizure, collection and acquisition of telephone communications  
21 information includes, but is not limited to, records indicating who each customer communicates  
22 with, at what time, and for how long. The aggregation of this information discloses the expressive,  
23 political, social, personal, private, and intimate associational connections among individuals and  
24 groups, which ordinarily would not be disclosed to the public or the government.

25           62.     Through the Associational Tracking Program, Defendants have seized, collected,  
26 acquired, and retained, and continue to seize, collect, acquire, and retain, bulk communications  
27 information of telephone calls made and received by Plaintiffs, their members, and their staffs. This  
28

1 information is otherwise private.

2 63. Because of the Associational Tracking Program, Plaintiffs have lost the ability to  
3 assure confidentiality in the fact of their communications to their members and constituent.  
4 Plaintiffs' associations and political advocacy efforts, as well as those of their members and staffs,  
5 are chilled by the fact that the Associational Tracking Program creates a permanent record of all of  
6 Plaintiffs' telephone communications with their members and constituents, among others.

7 64. Plaintiffs' associations and political advocacy efforts, as well as those of their  
8 members and staffs, are chilled by Defendants' search and analysis of information obtained through  
9 the Associational Tracking Program and Defendants' use and disclose of this information and the  
10 results of their searches and analyses.

11 65. Plaintiffs' telephone communications information obtained, retained, and searched  
12 pursuant to the Associational Tracking Program was at the time of acquisition, and at all times  
13 thereafter, neither relevant to an existing authorized criminal investigation nor to an existing  
14 authorized investigation to protect against international terrorism or clandestine intelligence  
15 activities.

16 66. Defendants' bulk seizure, collection, acquisition, and retention of the telephone  
17 communications information of Plaintiffs, their members, and their staffs is done without lawful  
18 authorization, probable cause, and/or individualized suspicion. It is done in violation of statutory and  
19 constitutional limitations and in excess of statutory and constitutional authority. Any judicial,  
20 administrative, or executive authorization (including any order issued pursuant to the business  
21 records provision of 50 U.S.C. § 1861) of the Associational Tracking Program or of the acquisition  
22 and retention of the communications information of Plaintiffs, their members, and their staffs is  
23 unlawful and invalid.

24 67. Defendants' bulk seizure, collection, acquisition, and retention of the telephone  
25 communications information of Plaintiffs, their members, and their staffs is done (a) without  
26 probable cause or reasonable suspicion to believe that Plaintiffs, their members, and their staffs have  
27 committed or are about to commit any crime or engage in any international terrorist activity; (b)

28

1 without probable cause or reasonable suspicion to believe that Plaintiffs, their members, or their  
2 staffs are foreign powers or agents of foreign powers; and (c) without probable cause or reasonable  
3 suspicion to believe that the communications of Plaintiffs, their members, and their staffs contain or  
4 pertain to foreign intelligence information, or relate to an investigation to obtain foreign intelligence  
5 information.

6 68. Defendants, and each of them, have authorized, approved, supervised, performed,  
7 caused, participated in, aided, abetted, counseled, commanded, induced, procured, enabled,  
8 contributed to, facilitated, directed, controlled, assisted in, or conspired in the Associational Tracking  
9 Program and in the seizure, collection, acquisition, and retention of the telephone communications  
10 information of Plaintiffs, their members, and their staffs. Defendants have committed these acts  
11 willfully, knowingly, and intentionally. Defendants continue to commit these acts and will continue  
12 to do so absent an order of this Court enjoining and restraining them from doing so.

#### 13 SEARCH

14 69. Through the Associational Tracking Program, Defendants have searched and continue  
15 to search communications information of telephone calls made and received by Plaintiffs, their  
16 members, and their staffs. Defendants use the communications information acquired for the  
17 Associational Tracking Program for a process known as “contact chaining” — the construction of an  
18 associational network graph that models the communication patterns of people, organizations, and  
19 their associates.

20 70. As part of the Associational Tracking Program, contact chains are created both in an  
21 automated fashion and based on particular queries. Contact chain analyses are typically performed  
22 for two degrees of separation (or two “hops”) away from an intended target. That is, an associational  
23 network graph would be constructed not just for the target of a particular query, but for any number  
24 in direct contact with that target, and any number in contact with a direct contact of the target.  
25 Defendants sometimes conduct associational analyses up to three degrees of separation (“three  
26 hops”) away.

27 71. The searches include Plaintiffs’ communications information even if plaintiffs are not  
28

1 targets of the government and even if they are not one, two or more “hops” away from a target. All  
2 telephone communications information is searched as part of the Associational Tracking Program.

3 72. Plaintiffs’ telephone communications information searched pursuant to the  
4 Associational Tracking Program was, at the time of search and at all times thereafter, was neither  
5 relevant to an existing authorized criminal investigation nor to an existing authorized investigation to  
6 protect against international terrorism or clandestine intelligence activities.

7 73. Defendants’ searching of the telephone communications information of Plaintiffs is  
8 done without lawful authorization, probable cause, and/or individualized suspicion. It is done in  
9 violation of statutory and constitutional limitations and in excess of statutory and constitutional  
10 authority. Any judicial, administrative, or executive authorization (including any business records  
11 order issued pursuant 50 U.S.C. § 1861) of the Associational Tracking Program or of the searching  
12 of the communications information of Plaintiffs is unlawful and invalid.

13 74. Defendants’ searching of the telephone communications information of Plaintiffs is  
14 done (a) without probable cause or reasonable suspicion to believe that Plaintiffs, their members, or  
15 their staffs, have committed or are about to commit any crime or engage in any international terrorist  
16 activity; (b) without probable cause or reasonable suspicion to believe that Plaintiffs, their members,  
17 or their staffs are foreign powers or agents of foreign powers; and (c) without probable cause or  
18 reasonable suspicion to believe that Plaintiffs’, their members’, or their staffs’ communications  
19 contain or pertain to foreign intelligence information or relate to an investigation to obtain foreign  
20 intelligence information.

21 75. Defendants, and each of them, have authorized, approved, supervised, performed,  
22 caused, participated in, aided, abetted, counseled, commanded, induced, procured, enabled,  
23 contributed to, facilitated, directed, controlled, assisted in, or conspired in the Associational Tracking  
24 Program and in the search or use of the telephone communications information of Plaintiffs, their  
25 members, and their staff. Defendants have committed these acts willfully, knowingly, and  
26 intentionally. Defendants continue to commit these acts and will continue to do so absent an order of  
27 this Court enjoining and restraining them from doing so.

28



**INJURY COMMON TO ALL PLAINTIFFS**

1  
2       76. Each and every Plaintiff is informed and believes that its associational activities have  
3 been harmed since the existence of the Associational Tracking Program became publicly known.  
4 Each Plaintiff has experienced a decrease in communications from members and constituents who  
5 had desired the fact of their communication to Plaintiff to remain secret, especially from the  
6 government and its various agencies, or has heard employees, members or associates express  
7 concerns about the confidentiality of the fact of their communications with Plaintiffs. Those  
8 Plaintiffs who operate hotlines have observed a decrease in calls to the hotlines and/or an increase in  
9 callers expressing concern about the confidentiality of the fact of their communications. Since the  
10 disclosure of the Associational Tracking Program, Plaintiffs have lost the ability to assure their  
11 members and constituents, as well as all others who seek to communicate with them, that the fact of  
12 their communications to Plaintiffs will be kept confidential, especially from the federal government,  
13 including its various agencies. This injury stems not from the disclosure of the Associational  
14 Tracking Program, but from the existence and operation of the program itself. Before the public  
15 disclosure of the program, Plaintiffs' assurances of confidentiality were illusory.

16       77. For instance, these specific Plaintiffs experienced the following:

17           (a) Plaintiff First Unitarian has a proud history of working for justice and  
18 protecting people in jeopardy for expressing their political views. In the 1950s, it resisted the  
19 McCarthy hysteria and supported blacklisted Hollywood writers and actors, and fought California's  
20 'loyalty oaths' all the way to the Supreme Court. And in the 1980s, it gave sanctuary to refugees from  
21 civil wars in Central America. The principles of its faith often require the church to take bold stands  
22 on controversial issues. Church members and neighbors who come to the church for help should not  
23 fear that their participation in the church might have consequences for themselves or their families.  
24 This spying makes people afraid to belong to the church community.

25           (b) Plaintiff Calguns Foundation runs a hotline for that allows the general public  
26 to call to ask questions about California's byzantine firearms laws. It has members who would be  
27 very worried about having their calls taped and stored by NSA/FBI when they're enquiring about  
28

1 whether firearms and parts they possess are felonious in California. It has a phone number  
2 specifically so people or their loved ones can call from jail because Californians are often arrested  
3 for actually innocent possession or use of firearms.

4 (c) Plaintiff NLG notes that much of its work involves cases (some high profile)  
5 involving individuals who have been charged with aiding terrorism or who have been monitored by  
6 the FBI and Joint Terrorism Task Forces for their political activism. Knowledge that its email and  
7 telephonic communications may likely be monitored has resulted in restricting what its employees  
8 and members say over the telephone and in email about legal advocacy and work related to NLG  
9 litigation or legal defense committees. In several instances, it has had to convene in-person meetings  
10 to discuss sensitive matters. One example is its "Green Scare" hotline for individuals contacted by  
11 the FBI, either as targets or in relation to environmental or animal rights cases. NLG immediately  
12 advises Hotline callers that the line may not be secure, asks limited information before referring  
13 callers to specific NLG attorneys in their geographic area, and does not keep notes or records of the  
14 calls. One foundation funder asks for records of Hotline calls, but in response the NLG can only send  
15 general examples of the types of calls it receives.

16 (d) Plaintiff Human Rights Watch conducts research and advocacy such that its  
17 effectiveness and credibility depend heavily on being able to interview those with direct knowledge  
18 of human rights abuses, be they victims, witnesses, perpetrators, or knowledgeable bystanders such  
19 as government officials, humanitarian agencies, lawyers and other civil society partners. Because  
20 this type of research and reporting can endanger people and organizations, our stakeholders—  
21 including even our researchers and/or consultants--often require us to keep their identities or other  
22 identifying information confidential. HRW has staff in these offices who talk to the above-  
23 mentioned types of stakeholders by telephone to conduct research. HRW is concerned that many of  
24 these stakeholders will have heightened concerns about contacting us through our offices now that  
25 we are aware the NSA is logging metadata of these calls. This impairs HRW's research ability  
26 and/or causes HRW to rely more on face-to-face encounters or other costly means of holding secure  
27 conversations.

28

1 (e) Plaintiff Shalom Center’s Executive Director, Rabbi Arthur Waskow, was  
2 subjected to COINTELPRO activity (warrantless searches, theft, forgery) by the FBI between 1968  
3 and 1974. He took part in a suit against the FBI and the Washington DC police (*Hobson v. Wilson*)  
4 for deprivation of the “right of the people peaceably to assemble.” Rabbi Waskow won in DC  
5 Federal District Court and the part of the suit that focused on the FBI was upheld in the DC Circuit  
6 Court of Appeals. The result of this experience is that he has been very troubled and frightened by  
7 the revelations of warrantless mass searches of telephone and Internet communications by the NSA.  
8 For several weeks, as the revelations continued, Rabbi Waskow realized the likelihood that the  
9 organization he leads, the Shalom Center, and he were under illegitimate surveillance and —  
10 because of its involvement in legal and nonviolent opposition to US government policy in several  
11 fields — possibly worse. This realization made him rethink whether he wanted to continue in sharp  
12 prophetic criticism and action in regard to disastrous public policies. Rabbi Waskow had trouble  
13 sleeping, delayed some essays and blogs he had been considering, and worried whether his actions  
14 might make trouble for nonpolitical relatives. Rabbi Waskow certainly felt a chill fall across his  
15 work of peaceable assembly, association, petition, and the free exercise of his religious convictions.

16 **COUNT I**

17 **Violation of First Amendment—Declaratory, Injunctive, and Other Equitable Relief**  
18 **(Against All Defendants)**

19 78. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
20 paragraphs of this complaint, as if set forth fully herein.

21 79. Plaintiffs, their members, and their staffs use telephone calls to communicate and to  
22 associate within their organization, with their members and with others, including to communicate  
23 anonymously and to associate privately.

24 80. By their acts alleged herein, Defendants have violated and are violating the First  
25 Amendment free speech and free association rights of Plaintiffs, their members, and their staffs,  
26 including the right to communicate anonymously, the right to associate privately, and the right to  
27 engage in political advocacy free from government interference.

28 81. By their acts alleged herein, Defendants have chilled and/or threaten to chill

1 the legal associations and speech of Plaintiffs, their members, and their staffs by, among other  
2 things, compelling the disclosure of their political and other associations, and eliminating Plaintiffs'  
3 ability to assure members and constituents that the fact of their communications with them will be  
4 kept confidential.

5 82. Defendants are irreparably harming Plaintiffs, their members, and their staffs by  
6 violating their First Amendment rights. Plaintiffs have no adequate remedy at law for Defendants'  
7 continuing unlawful conduct, and Defendants will continue to violate Plaintiffs' legal rights unless  
8 enjoined and restrained by this Court.

9 83. Plaintiffs seek that this Court declare that Defendants have violated the First  
10 Amendment rights of Plaintiffs, their members, and their staffs; enjoin Defendants, their agents,  
11 successors, and assigns, and all those in active concert and participation with them from violating the  
12 First Amendment to the United States Constitution; and award such other and further equitable relief  
13 as is proper.

## 14 **COUNT II**

### 15 **Violation of Fourth Amendment—Declaratory, Injunctive, and Equitable Relief** 16 **(Against All Defendants)**

17 84. Plaintiffs repeat and incorporate herein by reference the allegations in paragraphs 1  
18 through 66 of this complaint, as if set forth fully herein.

19 85. Plaintiffs have a reasonable expectation of privacy in their telephone communications,  
20 including in their telephone communications information.

21 86. By the acts alleged herein, Defendants have violated Plaintiffs' reasonable  
22 expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and  
23 seizures as guaranteed by the Fourth Amendment to the Constitution of the United States, including,  
24 but not limited to, obtaining *per se* unreasonable general warrants. Defendants have further violated  
25 Plaintiffs' rights by failing to apply to a court for, and for a court to issue, a warrant prior to any  
26 search and seizure as guaranteed by the Fourth Amendment.

27 87. Defendants are now engaging in and will continue to engage in the above-described  
28 violations of Plaintiffs' constitutional rights, and are thereby irreparably harming Plaintiffs.

1 Plaintiffs have no adequate remedy at law for Defendants' continuing unlawful conduct, and  
2 Defendants will continue to violate Plaintiffs' legal rights unless enjoined and restrained by this  
3 Court.

4 88. Plaintiffs seek that this Court declare that Defendants have violated their Fourth  
5 Amendment rights; enjoin Defendants, their agents, successors, and assigns, and all those in active  
6 concert and participation with them from violating the Plaintiffs' rights under the Fourth  
7 Amendment to the United States Constitution; and award such other and further equitable relief as is  
8 proper.

9 **COUNT III**

10 **Violation of Fifth Amendment—Declaratory, Injunctive, and Equitable Relief**  
11 **(Against All Defendants)**

12 89. Plaintiffs repeat and incorporate herein by reference the allegations in paragraphs 1  
13 through 66 of this complaint, as if set forth fully herein.

14 90. Plaintiffs, their members, and their staffs have an informational privacy interest in  
15 their telephone communications information, which reveals sensitive information about their  
16 personal, political, and religious activities and which Plaintiffs do not ordinarily disclose to the  
17 public or the government. This privacy interest is protected by state and federal laws relating to  
18 privacy of communications records and the substantive and procedural right to due process  
19 guaranteed by the Fifth Amendment.

20 91. Defendants through their Associational Tracking Program secretly seize, collect,  
21 acquire, retain, search, and use the bulk telephone communications information of Plaintiffs, their  
22 members, and their staff without providing notice to them, or process by which they could seek  
23 redress. Defendants provide no process adequate to protect their interests.

24 92. Defendants seize, collect, acquire, retain, search, and use the bulk telephone  
25 communications information of Plaintiffs, their members, and their staff without making any  
26 showing of any individualized suspicion, probable cause, or other governmental interest sufficient or  
27 narrowly tailored to justify the invasion of Plaintiffs' due process right to informational privacy.

28 93. Defendants seize, and acquire the bulk telephone communications information of

1 Plaintiffs, their members, and their staff under, *inter alia*, section 215 of the USA-PATRIOT Act (50  
2 U.S.C. § 1861).

3 94. On information and belief, Defendants' information seizure, collection and acquisition  
4 activities rely on a secret legal interpretation of 50 U.S.C. § 1861 under which bulk telephone  
5 communications information of persons generally is as a matter of law deemed a "tangible thing"  
6 "relevant" to "an investigation to obtain foreign intelligence information not concerning a United  
7 States person or to protect against international terrorism or clandestine intelligence activities," even  
8 without any particular reason to believe that telephone communications information is a "tangible  
9 thing" or that the telephone communications information of any particular person, including  
10 Plaintiffs, their members, and their staff, is relevant to an investigation to obtain foreign intelligence  
11 information not concerning a U.S. person or to protect against international terrorism or clandestine  
12 intelligence activities.

13 95. This legal interpretation of 50 U.S.C. § 1861 is not available to the general public,  
14 including Plaintiffs, their members, and their staff, leaving them and all other persons uncertain  
15 about where a reasonable expectation of privacy from government intrusion begins and ends and  
16 specifically what conduct may subject them to electronic surveillance.

17 96. This secret legal interpretation of 50 U.S.C. § 1861, together with provisions of the  
18 FISA statutory scheme that insulate legal interpretations from public disclosure and adversarial  
19 process, fails to establish minimal guidelines to govern law enforcement and/or intelligence seizure  
20 and collection.

21 97. The secret legal interpretation of 50 U.S.C. § 1861 used in the Associational Tracking  
22 Program and related surveillance programs causes section 1861 to be unconstitutionally vague in  
23 violation of the Fifth Amendment and the rule of law. The statute on its face gives no notice that it  
24 could be construed to authorize the bulk seizure and collection of telephone communications  
25 information for use in future investigations that do not yet exist.

26 98. By these and the other acts alleged herein, Defendants have violated and are  
27 continuing to violate the right to due process under the Fifth Amendment of Plaintiffs, their  
28

1 members, and their staff.

2 99. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs.

3 100. On information and belief, Defendants are now engaging in and will continue to  
4 engage in the above-described violations of Plaintiffs' constitutional rights, and are thereby  
5 irreparably harming Plaintiffs. Plaintiffs have no adequate remedy at law for Defendants' continuing  
6 unlawful conduct, and Defendants will continue to violate Plaintiffs' legal rights unless enjoined and  
7 restrained by this Court.

8 101. Plaintiffs seek that this Court declare that Defendants have violated their due process  
9 rights under the Fifth Amendment to the United States Constitution; enjoin Defendants, their agents,  
10 successors, and assigns, and all those in active concert and participation with them from violating the  
11 Plaintiffs' due process rights; and award such other and further equitable relief as is proper.

12 **COUNT IV**

13 **Violation of 50 U.S.C. § 1861—Declaratory, Injunctive and Other Equitable Relief**  
14 **(Against All Defendants)**

15 102. Plaintiffs repeat and incorporate herein by reference the allegations in paragraph 1  
16 through 66 of this complaint, as if set forth fully herein.

17 103. The business records order provision set forth in 50 U.S.C. § 1861 limits Defendants'  
18 ability to seek telephone communications information. It does not permit the suspicionless bulk  
19 seizure and collection of telephone communications information unconnected to any ongoing  
20 investigation. It does not permit an order requiring the production of intangible things, including  
21 telephone communications information not yet in existence.

22 104. Defendants' Associational Tracking Program and the seizure, collection, acquisition,  
23 retention, searching, and use of the telephone communications records of Plaintiffs, their members,  
24 and their staff exceed the conduct that may be lawfully authorized by an order issued under 50 U.S.C.  
25 § 1861.

26 105. By the acts alleged herein, Defendants are acting in excess of their statutory authority  
27 and in violation of the express statutory limitations and procedures Congress has imposed on them in  
28 50 U.S.C. § 1861.





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request that the Court:

1. Declare that the Program as alleged herein violates without limitation Plaintiffs' rights under the First, Fourth, and Fifth Amendments to the Constitution; and their statutory rights;
2. Award to Plaintiffs equitable relief, including without limitation, a preliminary and permanent injunction pursuant to the First, Fourth, and Fifth Amendments to the United States Constitution prohibiting Defendants' continued use of the Program, and a preliminary and permanent injunction pursuant to the First, Fourth, and Fifth Amendments requiring Defendants to provide to Plaintiffs an inventory of their communications, records, or other information that was seized in violation of the First, Fourth, and Fifth Amendments, and further requiring the destruction of all copies of those communications, records, or other information within the possession, custody, or control of Defendants.
3. Award to Plaintiffs reasonable attorneys' fees and other costs of suit to the extent permitted by law.
4. Order the return and destruction of their telephone communications information in the possession, custody, or control of Defendants, their agents, successors, and assigns, and all those in active concert and participation with them.
5. Grant such other and further relief as the Court deems just and proper.

DATED: September 10, 2013

Respectfully submitted,

/s/ Cindy Cohn  
 CINDY COHN  
 LEE TIEN  
 KURT OPSAHL  
 MATTHEW ZIMMERMAN  
 MARK RUMOLD  
 DAVID GREENE  
 JAMES S. TYRE  
 ELECTRONIC FRONTIER FOUNDATION

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

RICHARD R. WIEBE  
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III  
THE MOORE LAW GROUP

RACHAEL E. MENY  
MICHAEL S. KWUN  
BENJAMIN W. BERKOWITZ  
KEKER & VAN NEST, LLP

ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**JURY DEMAND**

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: September 10, 2013

Respectfully submitted,

/s/ Cindy Cohn  
CINDY COHN  
LEE TIEN  
KURT OPSAHL  
MATTHEW ZIMMERMAN  
MARK RUMOLD  
DAVID GREENE  
JAMES S. TYRE  
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE  
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III  
THE MOORE LAW GROUP

RACHAEL E. MENY  
MICHAEL S. KWUN  
BENJAMIN W. BERKOWITZ  
KEKER & VAN NEST, LLP

ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs

# Exhibit C

# Exhibit C

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

CAROLYN JEWEL *et al.*,

*Plaintiffs,*

v.

NATIONAL SECURITY AGENCY *et al.*,

*Defendants*

Case No. C:08-cv-4373-VRW

Chief Judge Vaughn R. Walker

~~PROPOSED~~ ORDER

Upon consideration of the parties' joint motion for entry of an order regarding the preservation of evidence and good cause appearing, the Court hereby ENTERS the following order based on the Court's prior Order of November 6, 2007, in 06-cv-1791-VRW (Dkt. 393).

A. The Court reminds all parties of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data and tangible things in the possession, custody and control of the parties to this action, and any employees, agents, contractors, carriers, bailees or other non-parties who possess materials reasonably anticipated to be subject to discovery in this action. Counsel are under an obligation to exercise efforts to identify and notify such non-parties, including employees of corporate or institutional parties.

B. "Documents, data and tangible things" is to be interpreted broadly to include writings, records, files, correspondence, reports, memoranda, calendars, diaries, minutes, electronic messages, voicemail, e-mail, telephone message records or logs, computer and network activity logs, hard drives, backup data, removable computer storage media such as tapes, disks and cards, printouts, document image files, web pages, databases, spreadsheets, software, books, ledgers, journals, orders, invoices, bills, vouchers, checks, statements, worksheets,

1 summaries, compilations, computations, charts, diagrams, graphic presentations, drawings, films,  
2 digital or chemical process photographs, video, phonographic, tape or digital recordings or  
3 transcripts thereof, drafts, jottings and notes. Information that serves to identify, locate, or link  
4 such material, such as file inventories, file folders, indices and metadata, is also included  
5 in this definition.

6 C. "Preservation" is to be interpreted broadly to accomplish the goal of maintaining the  
7 integrity of all documents, data and tangible things reasonably anticipated to be subject to  
8 discovery under FRCP 26, 45 and 56(e) in this action. Preservation includes taking reasonable  
9 steps to prevent the partial or full destruction, alteration, testing, deletion, shredding,  
10 incineration, wiping, relocation, migration, theft, or mutation of such material, as well as  
11 negligent or intentional handling that would make material incomplete or inaccessible.

12 D. Counsel are directed to inquire of their respective clients if the business or  
13 government practices of any party involve the routine destruction, recycling, relocation, or  
14 mutation of such materials and, if so, direct the party, to the extent practicable for the pendency  
15 of this order, either to

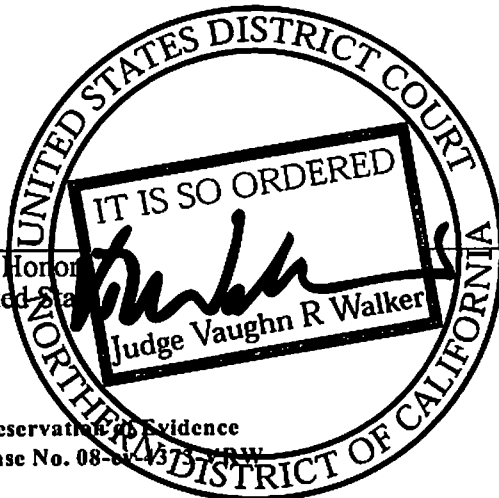
- 16 (1) halt such business or government practices;
  - 17 (2) sequester or remove such material from the business or government practices; or
  - 18 (3) arrange for the preservation of complete and accurate duplicates or copies of such
- 19 material, suitable for later discovery if requested.

20 Counsel representing each party shall, not later than December 15, 2009, submit to the  
21 Court under seal and pursuant to FRCP 11, a statement that the directive in paragraph D, above,  
22 has been carried out.

23 IT IS SO ORDERED.

24 Dated: Nov. 13, 2009.

25  
26 The Honorable  
United States



# Exhibit D

Exhibit D

United States District Court  
For the Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE: MDL Docket No 06-1791 VRW  
NATIONAL SECURITY AGENCY ORDER  
TELECOMMUNICATIONS RECORDS  
LITIGATION

This Document Relates To:  
ALL CASES

Plaintiffs have moved for an order prohibiting the alteration or destruction of evidence during the pendency of this action. MDL Doc # 384. The United States has filed papers opposing the motion, Doc # 386, and has prepared and lodged with the court a confidential submission designed for ex parte, in camera review. Doc # 387. Telephone company defendants AT&T, Cingular, Bellsouth, Sprint and Verizon have joined in the United States's opposition to plaintiffs' motion. Doc # 365, 388, 390.

Upon careful review of the non-confidential papers submitted in support of and in opposition to the motion, the court



1 has determined that (1) no hearing on the motion is necessary; (2)  
2 an order requiring the preservation of evidence is appropriate; and  
3 (3) an interim order shall forthwith enter requiring the parties to  
4 take steps to prevent the alteration or destruction of evidence as  
5 follows:

6           A. Until the issues in these proceedings can be further  
7 refined in light of the guidance and directives anticipated to be  
8 received upon appellate review of the court's decision in Hepting v  
9 AT&T Corporation, 439 F Supp 974 (N D Cal 2006) and of the Oregon  
10 district court's decision in Al-Haramain Islamic Foundation, Inc v  
11 Bush, 451 F Supp 2d 1215 (D Or 2006), the court reminds all parties  
12 of their duty to preserve evidence that may be relevant to this  
13 action. The duty extends to documents, data and tangible things in  
14 the possession, custody and control of the parties to this action,  
15 and any employees, agents, contractors, carriers, bailees or other  
16 non-parties who possess materials reasonably anticipated to be  
17 subject to discovery in this action. Counsel are under an  
18 obligation to exercise efforts to identify and notify such non-  
19 parties, including employees of corporate or institutional parties.

20           B. "Documents, data and tangible things" is to be  
21 interpreted broadly to include writings, records, files,  
22 correspondence, reports, memoranda, calendars, diaries, minutes,  
23 electronic messages, voicemail, e-mail, telephone message records  
24 or logs, computer and network activity logs, hard drives, backup  
25 data, removable computer storage media such as tapes, disks and  
26 cards, printouts, document image files, web pages, databases,  
27 spreadsheets, software, books, ledgers, journals, orders, invoices,  
28 bills, vouchers, checks, statements, worksheets, summaries,

1 compilations, computations, charts, diagrams, graphic  
2 presentations, drawings, films, digital or chemical process  
3 photographs, video, phonographic, tape or digital recordings or  
4 transcripts thereof, drafts, jottings and notes. Information that  
5 serves to identify, locate, or link such material, such as file  
6 inventories, file folders, indices and metadata, is also included  
7 in this definition.

8 C. "Preservation" is to be interpreted broadly to  
9 accomplish the goal of maintaining the integrity of all documents,  
10 data and tangible things reasonably anticipated to be subject to  
11 discovery under FRCP 26, 45 and 56(e) in this action. Preservation  
12 includes taking reasonable steps to prevent the partial or full  
13 destruction, alteration, testing, deletion, shredding,  
14 incineration, wiping, relocation, migration, theft, or mutation of  
15 such material, as well as negligent or intentional handling that  
16 would make material incomplete or inaccessible.

17 D. Counsel are directed to inquire of their respective  
18 clients if the business practices of any party involve the routine  
19 destruction, recycling, relocation, or mutation of such materials  
20 and, if so, direct the party, to the extent practicable for the  
21 pendency of this order, either to

- 22 (1) halt such business processes;  
23 (2) sequester or remove such material from the business  
24 process; or  
25 (3) arrange for the preservation of complete and accurate  
26 duplicates or copies of such material, suitable for later discovery  
27 if requested.

28 \\\

1           The most senior lawyer or lead trial counsel representing  
2 each party shall, not later than December 14, 2007, submit to the  
3 court under seal and pursuant to FRCP 11, a statement that the  
4 directive in paragraph D, above, has been carried out.

5           The clerk is directed to vacate the hearing now scheduled  
6 for November 15, 2007 in this matter.

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

IT IS SO ORDERED.



\_\_\_\_\_  
VAUGHN R WALKER  
United States District Chief Judge

United States District Court  
For the Northern District of California

# Exhibit E

# Exhibit E

Cindy Cohn <Cindy@eff.org>

March 10, 2014 8:35 AM



To: "Berman, Marcia (CIV)" <Marcia.Berman@usdoj.gov>

Cc: "Gilligan, Jim (CIV)" <James.Gilligan@usdoj.gov>, "wiebe@pacbell.net"

<wiebe@pacbell.net>, Stephanie Shattuck <steph@eff.org>, "Thomas E. Moore III

(tmoore@moorelawteam.com)" <tmoore@moorelawteam.com>, "Patton, Rodney (CIV)"

<Rodney.Patton@usdoj.gov>, "Dearinger, Bryan (CIV)" <Bryan.Dearinger@usdoj.gov>, "Ilann M.

Maazel" <imaazel@ecbalaw.com>

Re: Preservation of Evidence in Jewel v. NSA and First Unitarian Church v. NSA

Security:  Signed (cindy@eff.org)

Dear Marcy,

I am sorry that we did not hear from you after my message on Saturday asking for further clarification about how the government plans to ensure that it does not spoliage evidence. Unless we hear from you by noon California time today that the government does not intend to destroy evidence that may be likely to lead to the discovery of admissible evidence under the claims raised in Jewel and First Unitarian cases, we intend to seek a TRO from Judge White.

Please call or email me if you'd like to discuss this further. My cellphone is 415-307-2148. We have no desire to elevate this into an emergency matter before the court but believe we have no choice based upon the government's actions and statements so far.

Cindy

On Mar 8, 2014, at 11:43 AM, Cindy Cohn <Cindy@eff.org> wrote:

Dear Marcy,

Your response is confusing and troubling to us, as is your notice to the court in First Unitarian that you intend to begin to destroy call detail records on Tuesday, March 11, which is just two business days from now. To be clear, the only court that can relieve the government of its obligations to preserve evidence in our cases, regardless of the basis for those obligations, is the Northern District of California and it has not done so. This is true in Jewel and in First Unitarian.

As you know, both Jewel v. NSA and First Unitarian Church v. NSA arise from the ongoing bulk collection of telephone records, as did Hepting and the other MDL cases before that (along with additional information at issue in Jewel that must also be preserved). Neither the complaints nor the protective order mention the "President's Surveillance Program" so your reference to that program is confusing. The claims arise from the actual activity of bulk collection and state ongoing claims regardless of the legal or executive authority under which the government claims it conducts that activity at any point in time.

Duplicate

Cindy Cohn <Cindy@eff.org>

March 8, 2014 11:43 AM



To: "Berman, Marcia (CIV)" <Marcia.Berman@usdoj.gov>

Cc: "Gilligan, Jim (CIV)" <James.Gilligan@usdoj.gov>, "wiebe@pacbell.net" <wiebe@pacbell.net>, "Stephanie Shattuck" <steph@eff.org>, "Thomas E. Moore III (tmoore@moorelawteam.com)" <tmoore@moorelawteam.com>, "Patton, Rodney (CIV)" <Rodney.Patton@usdoj.gov>, "Dearinger, Bryan (CIV)" <Bryan.Dearinger@usdoj.gov>, "Ilann M. Maazel" <imaazel@ecbalaw.com>

Re: Preservation of Evidence in Jewel v. NSA

Security:  Signed (cindy@eff.org)

Dear Marcy,

Your response is confusing and troubling to us, as is your notice to the court in First Unitarian that you intend to begin to destroy call detail records on Tuesday, March 11, which is just two business days from now. To be clear, the only court that can relieve the government of its obligations to preserve evidence in our cases, regardless of the basis for those obligations, is the Northern District of California and it has not done so. This is true in Jewel and in First Unitarian.

As you know, both Jewel v. NSA and First Unitarian Church v. NSA arise from the ongoing bulk collection of telephone records, as did Hepting and the other MDL cases before that (along with additional information at issue in Jewel that must also be preserved). Neither the complaints nor the protective order mention the "President's Surveillance Program" so your reference to that program is confusing. The claims arise from the actual activity of bulk collection and state ongoing claims regardless of the legal or executive authority under which the government claims it conducts that activity at any point in time.

Moreover, we do not understand how the preservation order in place in Jewel (and Shubert) does not also include the preservation of the records at issue in First Unitarian. We further do not understand why the government failed to inform the FISC of your duties in Jewel and Shubert since they require you to preserve the same records or why it waited until just before the deadline to seek clarity on this issue, resulting in an apparent emergency situation that could easily have been avoided.

We will seek clarification from Judge White on this but we urge you not to destroy any records relevant to our claims in either case until we can do so. Please do provide us with full information so that we can narrow the issues before the court. Frankly, your email to me yesterday and filing in the First Unitarian case yesterday raise more concerns, not less, that the government has not been fulfilling its duties to preserve relevant evidence in either case. Please note that we will seek all available remedies if it turns out that the government has not abided by its duties.

Cindy

On Mar 7, 2014, at 6:14 PM, "Berman, Marcia (CIV)" <[Marcia.Berman@usdoj.gov](mailto:Marcia.Berman@usdoj.gov)> wrote:

Cindy -- In response to your questions regarding the preservation orders in Jewel (and the prior Hepting decision), the Government's motion to the FISC, and the FISC's decision today, addressed the recent litigation challenging the FISC-authorized telephony metadata collection under Section 215 -- litigation as to which there are no preservation orders. As we indicated last week, the Government's motion did not address the pending Jewel (and Shubert) litigation because the district court had previously entered preservation orders applicable to those cases. As we also indicated, since the entry of those orders the Government has complied with our preservation obligations in those cases. At the time the preservation issue was first litigated in the MDL proceedings in 2007, the Government submitted a classified ex parte, in camera declaration addressing in detail the steps taken to meet our preservation obligations. Because the activities undertaken in connection with the President's Surveillance Program (PSP) were not declassified until December 2013, we were not able to consult with you previously about the specific preservation steps that have been taken with respect to the Jewel litigation. However, the Government described for the district court in 2007 how it was meeting its preservation obligations, including with respect to the information concerning the PSP activities declassified last December. We have been working with our clients to prepare an unclassified summary of the preservation steps described to the court in 2007 so that we can address your questions in an orderly fashion with Judge White, if you continue to believe that is necessary.

Thanks -- Marcy

---

**From:** Berman, Marcia (CIV)

**Sent:** Friday, March 07, 2014 6:14 PM

**To:** Cindy Cohn

**Cc:** Gilligan, Jim (CIV); [wiebe@pacbell.net](mailto:wiebe@pacbell.net); Stephanie Shattuck; Thomas E. Moore III ([tmoores@moorelawteam.com](mailto:tmoores@moorelawteam.com)); Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel

**Subject:** FW: Preservation of Evidence in Jewel v. NSA

Cindy -- we'll get back to you on this today, hopefully within an hour. Thanks -- Marcy

---

**From:** Dearing, Bryan (CIV)

**Sent:** Friday, March 07, 2014 4:39 PM

**To:** Berman, Marcia (CIV)

**Subject:** FW: Preservation of Evidence in Jewel v. NSA

FYI ...

---

**From:** Cindy Cohn [<mailto:cindy@eff.org>]

**Sent:** Friday, March 07, 2014 4:37 PM

**To:** Gilligan, Jim (CIV)

**Cc:** Rick Wiebe; Stephanie Shattuck; Thomas E. Moore III; Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel

**Subject:** Re: Preservation of Evidence in Jewel v. NSA

Hi Jim,

I assume you've seen the FISC Order. Can you please explain how the court could be under the misimpression that there are no preservation orders for the telephone records information in place given the history at Jewel and Hepting before it? As you might expect, this is quite alarming to us.

We will be filing something shortly and I want to be sure that we correctly state your position.

Cindy

Sent from my phone

On Feb 28, 2014, at 5:17 PM, Cindy Cohn <[cindy@eff.org](mailto:cindy@eff.org)> wrote:

Hi Jim,

We'll wait a bit, assuming this doesn't drag on too long. Thanks for responding.

Cindy

Sent from my phone

On Feb 28, 2014, at 5:26 PM, "Gilligan, Jim (CIV)" <[James.Gilligan@usdoj.gov](mailto:James.Gilligan@usdoj.gov)> wrote:

Cindy,

We did receive your email about preservation, and I wanted to get back to you before the week ended to let you know that we will need a bit more time to prepare a more complete response than we will be able to do by Monday. So I would ask that you forbear from filing anything with the FISC, or Judge White, until we have further opportunity to confer. As you noted, *Jewel* and *Shubert* are not specifically mentioned in the motion we filed with the FISC, but as you also observed, the question of preservation has already been litigated in those cases, and the court issued separate preservation orders that govern there. Many of the details surrounding the intelligence programs in question remain classified, however, and so there remain limitations on our ability to confer with you concerning our compliance with those orders.

At this point I need to consult further with my clients to ascertain how much information I can convey to you about the Government's preservation efforts without revealing classified information. I simply won't be in a position to provide you with a detailed response to your



inquiry by Monday, as you request, in part because of the work that remains on our reply to your brief on the court's four questions, and in part because I will be out of the office on Monday and Tuesday for a family ski trip. (Also, as you observed, Marcy is presently diverted by another matter.) But we will do our best to address your questions by the middle of next week.

JG

James J. Gilligan  
Special Litigation Counsel  
Civil Division, Federal Programs Branch  
U.S. Department of Justice  
P.O. Box 883  
Washington, D.C. 20044

Tel: 202-514-3358

---

**From:** Cindy Cohn [<mailto:cindy@eff.org>]  
**Sent:** Friday, February 28, 2014 5:54 PM  
**To:** Gilligan, Jim (CIV)  
**Cc:** Rick Wiebe; Stephanie Shattuck; Thomas E. Moore III; Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel  
**Subject:** Re: Preservation of Evidence in Jewel v. NSA

Hi Jim, Rodney and Bryan,

I just wanted to confirm that you received this and learn when you will be responding.

We are planning to file something in the FISC and before Judge Walker early next week and I do want to be able to accurately convey your position.

Thanks,

Cindy

On Feb 26, 2014, at 4:08 PM, Cindy Cohn <[Cindy@eff.org](mailto:Cindy@eff.org)> wrote:

Hi Jim,

Rick will write you separately about the scheduling, but I wanted to raise something that has confused us and to seek clarification.

We saw your filing in the FISC asking that the Court's current Primary Order be amended to authorize the preservation and/or storage of call detail records beyond five years based upon your duty to preserve evidence and mentioning the First Unitarian case specifically. We do agree that the government has a duty to preserve all reasonably anticipated to be subject to discovery in this action. We were surprised, however, that you did not approach us to discuss ways that this duty could be met short of the request you made, which we read as allowing you to preserve all of the metadata you have collected.

We also write because, as I think you know, the government has been under an obligation to preserve telephone records it has collected since 2006, when the cases that made up the MDL action In Re NSA were first filed. One of those cases, Shubert v. Obama, has remained ongoing since that time. That obligation was reinforced by an Order issued by Judge Walker in 2007 and order was specifically adopted by the court in Jewel v. NSA in 2009 by a joint request by the government and the plaintiffs (Jewel v. NSA, Doc. 51).

Thus my confusion. I'm not sure why the Jewel (and Shubert) cases were not mentioned or referenced in the request to the FISC since both of those also contain ongoing preservation obligations related to the bulk phone records collection by the NSA. Since they were not, it also raises the question of whether and how the government has been abiding by its obligation to preserve evidence in those two cases, since obviously both have been pending for more than five years.

I would appreciate a prompt response and clarification. I'm confident that the government takes seriously its obligation to preserve evidence that may be relevant to pending litigation, but given the situation, I would like a specific reaffirmation that bulk telephone records collected by the NSA have been preserved in the Jewel case and I suspect Ilann is concerned about the same for Shubert. I would also request some more specific information about how that preservation has occurred -- similar to the plan you suggested to the FISC in your motion.

I hope you can provide us with a thorough response before any additional phone records are destroyed and hopefully by Monday, March 3. While we're hopeful that we will receive a satisfactory response, but if not, we do intend to raise this question with both the FISC and the Judge White.

Thanks,

Cindy

PS: Has Marcy gone? I noticed that she's not on the pleadings you filed last week or on this message.

-----  
Cindy Cohn  
Legal Director  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333 x108  
---Cindy@eff.org  
---www.eff.org

Join EFF! <https://supporters.eff.org/donate>

-----  
Cindy Cohn  
Legal Director  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333 x108  
---Cindy@eff.org  
---www.eff.org

Join EFF! <https://supporters.eff.org/donate>

1 CINDY COHN (SBN 145997)  
cindy@eff.org  
2 LEE TIEN (SBN 148216)  
KURT OPSAHL (SBN 191303)  
3 JAMES S. TYRE (SBN 083117)  
MARK RUMOLD (SBN 279060)  
4 ANDREW CROCKER (SBN 291596)  
ELECTRONIC FRONTIER FOUNDATION  
5 815 Eddy Street  
San Francisco, CA 94109  
6 Telephone: (415) 436-9333  
Fax: (415) 436-9993

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

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

THOMAS E. MOORE III (SBN 115107)  
tmoore@rroysclaw.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

11  
12  
13  
14 *Counsel for Plaintiffs*

15  
16 **UNITED STATES DISTRICT COURT**  
17 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
18 **SAN FRANCISCO DIVISION**

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

) CASE NO. 08-CV-4373-JSW  
)  
)  
) **[PROPOSED] TEMPORARY**  
) **RESTRAINING ORDER**  
)  
) Hon. Jeffrey S. White  
) Courtroom 11 - 19th Floor

1 This matter is before the Court on plaintiffs’ motion for a temporary restraining order to  
2 prevent defendants National Security Agency, United States of America, Department of Justice,  
3 Barack H. Obama, Keith B. Alexander, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their  
4 official capacities) (collectively, the “government defendants”) and all those in active concert or  
5 participation with them from destroying any potential evidence relevant to the claims at issue in  
6 this action, including but not limited to prohibiting the destruction of any telephone metadata or  
7 “call detail” records. The government defendants have given notice that they will commence  
8 destroying call detail records on Tuesday morning, March 11, 2014. ECF No. 85 in *First*  
9 *Unitarian Church of Los Angeles v. NSA*, No. 13-cv-3287-JSW.

10 Plaintiffs contend that the Court’s prior evidence preservation order (ECF No. 51) as well  
11 as defendants’ obligations under the Federal Rules of Civil Procedure prohibit destruction of this  
12 potential evidence. It is undisputed that the Court would be unable to afford effective relief to  
13 plaintiffs once the records are destroyed, and therefore the harm plaintiffs face is irreparable. A  
14 temporary restraining order is necessary and appropriate so that the Court may decide whether the  
15 evidence should be preserved with the benefit of full briefing and participation by all parties.

16 It is hereby ordered that defendants National Security Agency, United States of America,  
17 Department of Justice, Barack H. Obama, Keith B. Alexander, Eric H. Holder, Jr., and James R.  
18 Clapper, Jr. (in their official capacities), their officers, agents, servants, employees, and attorneys,  
19 and all those in active concert or participation with them are prohibited, enjoined, and restrained  
20 from destroying any potential evidence relevant to the claims at issue in this action, including but  
21 not limited to prohibiting the destruction of any telephone metadata or “call detail” records,  
22 pending further order of the Court.

23 The Court sets the following briefing and hearing schedule in this matter:

24	Plaintiffs’ opening brief	_____
25	Government defendants opposition brief	_____
26	Plaintiffs’ reply brief	_____
27	Hearing	_____

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

This order expires at \_\_\_\_\_.

Entered at \_\_\_\_ a.m./p.m. on March \_\_\_\_, 2014

IT IS SO ORDERED.

\_\_\_\_\_  
UNITED STATES DISTRICT JUDGE

1 CINDY COHN (SBN 145997)  
 cindy@eff.org  
 2 LEE TIEN (SBN 148216)  
 3 KURT OPSAHL (SBN 191303)  
 MATTHEW ZIMMERMAN (SBN 212423)  
 4 MARK RUMOLD (SBN 279060)  
 DAVID GREENE (SBN 160107)  
 5 JAMES S. TYRE (SBN 083117)  
 ELECTRONIC FRONTIER FOUNDATION  
 6 815 Eddy Street  
 San Francisco, CA 94109  
 7 Tel.: (415) 436-9333; Fax: (415) 436-9993  
 8  
 THOMAS E. MOORE III (SBN 115107)  
 9 tmoore@rroyselaw.com  
 ROYSE LAW FIRM, PC  
 10 1717 Embarcadero Road  
 Palo Alto, CA 94303  
 11 Tel.: 650-813-9700; Fax: 650-813-9777

12 *Counsel for Plaintiffs*

RACHAEL E. MENY (SBN 178514)  
 rmeny@kvn.com  
 MICHAEL S. KWUN (SBN 198945)  
 BENJAMIN W. BERKOWITZ (SBN 244441)  
 KEKER & VAN NEST, LLP  
 633 Battery Street  
 San Francisco, California 94111  
 Tel.: (415) 391-5400; Fax: (415) 397-7188

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

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

14 **UNITED STATES DISTRICT COURT**  
 15 **NORTHERN DISTRICT OF CALIFORNIA**  
 16 **SAN FRANCISCO DIVISION**

17 FIRST UNITARIAN CHURCH OF LOS  
 18 ANGELES, *et al.*,  
 19 **Plaintiffs,**  
 20 **v.**  
 21 NATIONAL SECURITY AGENCY, *et al.*,  
 22 **Defendants.**

Case No: 3:13-cv-03287 JSW

**PLAINTIFFS' NOTICE OF EX  
 PARTE MOTION AND EX PARTE  
 MOTION FOR A TEMPORARY  
 RESTRAINING ORDER TO  
 PREVENT THE GOVERNMENT  
 FROM DESTROYING EVIDENCE**

Date: March 10, 2014  
 Time: 1:30 p.m.  
 Courtroom 11, 19th Floor  
 The Honorable Jeffrey S. White

26 **IMMEDIATE RELIEF REQUESTED**  
 27 **CRITICAL DATE: TUESDAY MORNING, MARCH 11, 2014**

1 **NOTICE OF EX PARTE MOTION**

2 PLEASE TAKE NOTICE that on Monday, March 10, 2014 at 1:30 p.m., or as soon  
3 thereafter as they may be heard by the Court at Courtroom 11, 19th Floor, 450 Golden Gate Ave.,  
4 San Francisco, CA, plaintiffs will move ex parte for a temporary restraining order and, after a  
5 hearing has been held, an order prohibiting, enjoining, and restraining defendants National Security  
6 Agency, United States of America, Department of Justice, Barack H. Obama, Keith B. Alexander,  
7 Eric H. Holder, Jr., and James R. Clapper, Jr. (in their official capacities) (collectively, the  
8 “government defendants”) and all those acting in concert with them from destroying any evidence  
9 relevant to the claims at issue in this action, including but not limited to prohibiting the destruction  
10 of any telephone metadata or “call detail” records.

11 Notice of this motion has been given to opposing counsel. Attached to the Cohn Declaration  
12 filed herewith as Exhibit E are email exchanges between parties’ counsel between on February 26,  
13 2014, and this morning, March 10, 2014, in which plaintiffs have consistently stated their intentions  
14 to seek relief from this court unless the government clarifies its intention to preserve all relevant  
15 evidence in the two cases consistent with its obligations in both cases and the preservation order in  
16 *Jewel v. NSA* that reaches the same telephonic records at issue in *First Unitarian Church v. NSA*.

17 This matter became an emergency matter because on Friday, March 7, based on a mistaken  
18 belief that no preservation order existed for the material at issue, and without consultation with  
19 plaintiff or this Court, the FISC denied the government’s motion to be allowed to preserve the  
20 telephone records it had collected. Late Friday, the government served notice in the *First Unitarian*  
21 case that it intended to begin destroying the records.

22 **REASONS WHY RELIEF SHOULD BE GRANTED**

23 The government defendants have given notice that they plan to begin destroying telephone  
24 metadata (“call detail record”) evidence relevant to this lawsuit tomorrow, **Tuesday Morning,**  
25 **March 11, 2014.** ECF No. 85 in *First Unitarian v. NSA*, No. 13-cv-3287-JSW. Plaintiffs  
26 respectfully request that the Court **today** issue an immediate temporary restraining order to prevent  
27 the destruction of evidence before the Court has an opportunity to determine whether destruction of  
28



1 this evidence is contrary to the Court's November 16, 2009 evidence preservation order (ECF  
2 No. 51) or otherwise contrary to the government defendants' discovery obligations.

3 The purpose of a TRO is to preserve the status quo and prevent irreparable harm "just so long  
4 as is necessary to hold a hearing, and no longer." *Granny Goose Foods, Inc. v. Brotherhood of*  
5 *Teamsters*, 415 U.S. 423, 439 (1974). This is exactly what is needed here.

6 There has been litigation challenging the lawfulness of the government's telephone metadata  
7 collection activity, Internet metadata collection activity, and upstream collection activity pending in  
8 the Northern District of California continuously since 2006. The government has been under  
9 evidence preservation orders in those lawsuits continuously since 2007.

10 The first-filed case was *Hepting v. AT&T*, No. 06-cv-0672 (N.D. Cal). It became the lead  
11 case in the MDL proceeding in this district, *In Re: National Security Agency Telecommunications*  
12 *Records Litigation*, MDL No. 06-cv-1791-VRW (N.D. Cal). On November 6, 2007, this Court  
13 entered an evidence preservation order in the MDL proceeding. ECF No. 393 in MDL No. 06-cv-  
14 1791-VRW. One of the MDL cases, *Virginia Shubert, et al., v. Barack Obama, et al.* No. 07-cv-  
15 0603-JSW (N.D. Cal.), remains in litigation today before this Court, and the MDL preservation order  
16 remains in effect today as to that case.

17 In 2008, movants filed this action—*Jewel v. NSA*—and this Court related it to the *Hepting*  
18 action. This Court entered an evidence preservation order in *Jewel*. ECF No. 51. The *Jewel*  
19 evidence preservation order remains in effect as of today.

20 The government has never sought to seek clarification of its preservation obligations  
21 regarding telephone metadata records from this Court or raised the issue with plaintiffs. Instead, the  
22 government defendants chose to raise the issue of preservation of telephone metadata records in an  
23 ex parte proceeding before the Foreign Intelligence Surveillance Court, without any notice to  
24 plaintiffs and without mentioning its obligations with regard to the same telephone records in *Jewel*  
25 *v. NSA* and *Shubert v. Obama*. Plaintiffs learned of the government's motion by reading the news  
26 media, and asked counsel for the government defendants to explain why they had not told the FISC  
27 about the *Jewel* evidence preservation order. See Cohn Decl, Exh. E.

28

1           Indeed, the government is aware and has acknowledged that destruction of the information in  
2 question may conflict with the preservation orders issued in this and related cases: “While the  
3 Court’s Primary Order requires destruction of the BR metadata no longer than five years (60 months)  
4 after its initial collection, such destruction could be inconsistent with the Government’s preservation  
5 obligations in connection with civil litigation pending against it. Accordingly, to avoid the  
6 destruction of the BR metadata, the Government seeks an amendment to the Court’s Primary Order  
7 that would allow the NSA to preserve and/or store the BR metadata for non-analytic purposes until  
8 relieved of its preservation obligations, or until further order of this Court under the conditions  
9 described below.” Government’s Motion for Second Amendment to Primary Order, FISC No. BR  
10 14-01 (February 25, 2014). Although the government’s motion in the FISC did not discuss the  
11 preservation order in *Jewel*, this preservation order includes *the same* records at issue in *First*  
12 *Unitarian*.

### 13                           LEGAL STANDARD FOR TEMPORARY RESTRAINING ORDER

14           “A plaintiff seeking a [TRO] must establish that he is likely to succeed on the merits, that he  
15 is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities  
16 tips in his favor, and that an injunction is in the public interest.” *Network Automation, Inc. v.*  
17 *Advanced Sys. Concepts*, 638 F.3d 1137, 1144 (9th Cir. 2011) (quoting *Winter v. Natural Res.*  
18 *Defense Council, Inc.*, 555 U.S. 7 (2008)).

#### 19           A.     Likelihood of Success

20           The *Jewel* preservation order required the Government to “preserve evidence that may be  
21 relevant to this action.” The *Jewel* complaint alleged unlawful and unconstitutional acquisition of  
22 call-detail records, including the “call-detail records collected under the National Security Agency  
23 (NSA) bulk telephony metadata program” that the Government proposed to destroy.

24           Plaintiffs sought, among other relief, an injunction “requiring Defendants to provide to  
25 Plaintiffs and the class an inventory of their communications, records, or other information that was  
26 seized in violation of the Fourth Amendment.” Complaint, Prayer for Relief. This would be  
27 impossible if the records are destroyed. While the Plaintiff ultimately want the call-detail records  
28

1 destroyed at the conclusion of the case, there is no doubt the call-records “may be relevant” in the  
2 interim.

3 The Jewel order also required the Government to cease “destruction, recycling, relocation, or  
4 mutation of such materials.” Thus, the proposed destruction would be in direct violation of the  
5 Jewel preservation order.

6 **B. Irreparable Harm**

7 If the government proceeds with its planned destruction of evidence, the evidence will be  
8 gone. This is by definition irreparable.

9 **C. Balance of Equities**

10 While the Government contends it is required by the FISC to destroy the records  
11 immediately, the FISC order belies this assertion. The FISC denied the government's motion  
12 without prejudice to bringing another motion with additional facts and the FISC plainly was not  
13 informed of the preservation order in Jewel or even of its existence. The FISC clearly contemplated  
14 that the evidence destruction could wait while the government prepared and filed another motion,  
15 and continue until the Court considered and ruled on the motion.

16 **D. Public Interest**

17 These records are both an affront to the rights of millions of Americans and proof of their  
18 violation. Plaintiffs have no objection to severe restrictions on the Government’s right to access and  
19 use the information, which will address the public interest in the documents being destroyed.  
20 However, it remains in the public interest to wait a short period of time before taking action, so that  
21 the fate of the documents can be addressed in an orderly fashion.

22 The necessity for this ex parte application could have been easily avoided had the  
23 government defendants followed the discovery and evidence preservation practices customary in this  
24 District. They could have, but did not, raised the issue of preserving telephone metadata records in  
25 the CMC statement meet-and-confer process in September 2013 (three months after the government  
26 defendants publicly acknowledged the phone records program), or at the Case Management  
27 Conference itself on September 27, 2013. They could have, but did not, raised this issue in the CMC  
28



1 CINDY COHN (SBN 145997)  
 2 cindy@eff.org  
 3 LEE TIEN (SBN 148216)  
 4 KURT OPSAHL (SBN 191303)  
 5 MATTHEW ZIMMERMAN (SBN 212423)  
 6 MARK RUMOLD (SBN 279060)  
 7 DAVID GREENE (SBN 160107)  
 8 JAMES S. TYRE (SBN 083117)  
 9 ANDREW CROCKER (SBN 291596)  
 10 ELECTRONIC FRONTIER FOUNDATION  
 11 815 Eddy Street  
 12 San Francisco, CA 94109  
 13 Tel.: (415) 436-9333; Fax: (415) 436-9993  
 14 THOMAS E. MOORE III (SBN 115107)  
 15 tmoore@troyselaw.com  
 16 ROYSE LAW FIRM, PC  
 17 1717 Embarcadero Road  
 18 Palo Alto, CA 94303  
 19 Tel.: 650-813-9700; Fax: 650-813-9777  
 20 Counsel for Plaintiffs

RACHAEL E. MENY (SBN 178514)  
 rmeny@kvn.com  
 MICHAEL S. KWUN (SBN 198945)  
 BENJAMIN W. BERKOWITZ (SBN 244441)  
 KEKER & VAN NEST, LLP  
 633 Battery Street  
 San Francisco, California 94111  
 Tel.: (415) 391-5400; Fax: (415) 397-7188  
 RICHARD R. WIEBE (SBN 121156)  
 wiebe@pacbell.net  
 LAW OFFICE OF RICHARD R. WIEBE  
 One California Street, Suite 900  
 San Francisco, CA 94111  
 Tel.: (415) 433-3200; Fax: (415) 433-6382  
 ARAM ANTARAMIAN (SBN 239070)  
 aram@eff.org  
 LAW OFFICE OF ARAM ANTARAMIAN  
 1714 Blake Street  
 Berkeley, CA 94703  
 Telephone: (510) 289-1626

14 **UNITED STATES DISTRICT COURT**  
 15 **NORTHERN DISTRICT OF CALIFORNIA**  
 16 **SAN FRANCISCO DIVISION**

18 **FIRST UNITARIAN CHURCH OF LOS**  
 19 **ANGELES, et al.**  
 20 **Plaintiffs,**  
 21 **v.**  
 22 **NATIONAL SECURITY AGENCY, et al.,**  
 23 **Defendants.**

Case No: 3:13-cv-03287 JSW  
**DECLARATION OF CINDY COHN**  
 Courtroom 11, 19th Floor  
 The Honorable Jeffrey S. White

1 I, CINDY COHN, hereby declare:

2 1. I am a lawyer duly licensed to practice law in the State of California and before this  
3 district. I am the Legal Director of the Electronic Frontier Foundation, counsel of record for the  
4 plaintiffs.

5 2. I have attached to this Declaration true and correct copies of the following  
6 documents:

- 7 • **Exhibit A:** Complaint for Constitutional and Statutory Violations, Seeking  
8 Damages, Declaratory and Injunctive Relief in *Carolyn Jewel, et al., v. National*  
9 *Security Agency, et al.*, No. 08-cv-4373-JSW (N.D. Cal.) filed September 18, 2008;
- 10 • **Exhibit B:** First Amended Complaint for Constitutional and Statutory Violations,  
11 Seeking Declaratory and Injunctive Relief in *First Unitarian Church of Los Angeles,*  
12 *et al. v. National Security Agency, et al.*, Case No. 13-cv-3287-JSW (N.D. Cal.) filed  
13 on March 7, 2014;
- 14 • **Exhibit C:** Evidence Preservation Order in *Carolyn Jewel, et al., v. National*  
15 *Security Agency, et al.*, No. 08-cv-4373-JSW (N.D. Cal.) filed November 16, 2009;
- 16 • **Exhibit D:** Evidence Preservation Order in *In Re: National Security Agency*  
17 *Telecommunications Records Litigation*, MDL No. 06-cv-1791-VRW (N.D. Cal)  
18 dated November 6, 2007; and
- 19 • **Exhibit E:** Emails between plaintiffs and defendants regarding preservation  
20 issues.

21 I declare under penalty of perjury under the laws of the United States that the foregoing is  
22 true and correct. Executed on March 10, 2014, at San Francisco, California.

23  
24  
25  
26  
27  
28

/s/ Cindy Cohn  
CINDY COHN

# Exhibit A

# Exhibit A

1 ELECTRONIC FRONTIER FOUNDATION  
CINDY COHN (145997)  
2 cindy@eff.org  
LEE TIEN (148216)  
3 KURT OPSAHL (191303)  
KEVIN S. BANKSTON (217026)  
4 JAMES S. TYRE (083117)  
454 Shotwell Street  
5 San Francisco, CA 94110  
Telephone: 415/436-9333; Fax: 415/436-9993  
6

RICHARD R. WIEBE (121156)  
7 wiebe@pacbell.net  
LAW OFFICE OF RICHARD R. WIEBE  
8 425 California Street, Suite 2025  
San Francisco, CA 94104  
9 Telephone: 415/433-3200; Fax: 415/433-6382

10 THOMAS E. MOORE III (115107)  
tmoore@moorelawteam.com  
11 THE MOORE LAW GROUP  
228 Hamilton Avenue, 3rd Floor  
12 Palo Alto, CA 94301  
Telephone: 650/798-5352; Fax: 650/798-5001  
13

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

16 CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS,  
ERIK KNUTZEN and JOICE WALTON, on behalf of  
17 themselves and all others similarly situated,

18 Plaintiffs,

19 vs.

20 NATIONAL SECURITY AGENCY and KEITH B.  
ALEXANDER, its Director, in his official and personal  
21 capacities; MICHAEL V. HAYDEN, in his personal capacity;  
the UNITED STATES OF AMERICA; GEORGE W. BUSH,  
22 President of the United States, in his official and personal  
capacities; RICHARD B. CHENEY, in his personal capacity;  
23 DAVID S. ADDINGTON, in his personal capacity;  
DEPARTMENT OF JUSTICE and MICHAEL B.  
24 MUKASEY, its Attorney General, in his official and personal  
capacities; ALBERTO R. GONZALES, in his personal  
25 capacity; JOHN D. ASHCROFT, in his personal capacity;  
JOHN M. MCCONNELL, Director of National Intelligence, in  
26 his official and personal capacities; JOHN D. NEGROPONTE,  
in his personal capacity; and DOES #1-100, inclusive,  
27

28 Defendants.

ORIGINAL  
FILED

SEP 18 2008

RICHARD W. WIEKING  
CLERK, U.S. DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

E-Filed

CASE NO:

CLASS ACTION

COMPLAINT FOR  
CONSTITUTIONAL AND  
STATUTORY  
VIOLATIONS, SEEKING  
DAMAGES,  
DECLARATORY, AND  
INJUNCTIVE RELIEF

CRB

DEMAND FOR JURY  
TRIAL





1           7.     In addition to eavesdropping on or reading specific communications, Defendants  
2 have indiscriminately intercepted the communications content and obtained the communications  
3 records of millions of ordinary Americans as part of the Program authorized by the President.

4           8.     The core component of the Program is Defendants' nationwide network of  
5 sophisticated communications surveillance devices, attached to the key facilities of  
6 telecommunications companies such as AT&T that carry Americans' Internet and telephone  
7 communications.

8           9.     Using this shadow network of surveillance devices, Defendants have acquired and  
9 continue to acquire the content of a significant portion of the phone calls, emails, instant messages,  
10 text messages, web communications and other communications, both international and domestic,  
11 of practically every American who uses the phone system or the Internet, including Plaintiffs and  
12 class members, in an unprecedented suspicionless general search through the nation's  
13 communications networks.

14           10.    In addition to using surveillance devices to acquire the domestic and international  
15 communications content of millions of ordinary Americans, Defendants have unlawfully solicited  
16 and obtained from telecommunications companies such as AT&T the complete and ongoing  
17 disclosure of the private telephone and Internet transactional records of those companies' millions  
18 of customers (including communications records pertaining to Plaintiffs and class members),  
19 communications records indicating who the customers communicated with, when and for how long,  
20 among other sensitive information.

21           11.    This non-content transactional information is analyzed by computers in conjunction  
22 with the vast quantity of communications content acquired by Defendants' network of surveillance  
23 devices, in order to select which communications are subjected to personal analysis by staff of the  
24 NSA and other Defendants, in what has been described as a vast "data-mining" operation.  
25  
26  
27  
28



1 claims on the NSA and the Department of Justice on December 19, 2007, and over six months have  
2 passed since the filing of that notice.

3 **PARTIES**

4 20. Plaintiff Tash Hepting, a senior systems architect, is an individual residing in  
5 Livermore, California. Hepting has been a subscriber and user of AT&T's residential long distance  
6 telephone service since at least June 2004.

7  
8 21. Plaintiff Gregory Hicks is an individual residing in San Jose, California. Hicks, a  
9 retired Naval Officer and systems engineer, has been a subscriber and user of AT&T's residential  
10 long distance telephone service since February 1995.

11 22. Plaintiff Carolyn Jewel is an individual residing in Petaluma, California. Jewel, a  
12 database administrator and author, has been a subscriber and user of AT&T's WorldNet dial-up  
13 Internet service since approximately June 2000.

14  
15 23. Plaintiff Erik Knutzen is an individual residing in Los Angeles, California. Knutzen,  
16 a photographer and land use researcher, was a subscriber and user of AT&T's WorldNet dial-up  
17 Internet service from at least October 2003 until May 2005. Knutzen is currently a subscriber and  
18 user of AT&T's High Speed Internet DSL service.

19 24. Plaintiff Joice Walton is an individual residing in San Jose, California. Walton, a  
20 high technology purchasing agent, is a current subscriber and user of AT&T's WorldNet dial-up  
21 Internet service. She has subscribed to and used this service since around April 2003.

22 25. Defendant National Security Agency (NSA) is an agency under the direction and  
23 control of the Department of Defense that collects, processes and disseminates foreign signals  
24 intelligence. It is responsible for carrying out the Program challenged herein.

25 26. Defendant Lieutenant General Keith B. Alexander is the current Director of the NSA,  
26 in office since April 2005. As NSA Director, defendant Alexander has ultimate authority for  
27 supervising and implementing all operations and functions of the NSA, including the Program.  
28

1           27.     Defendant Lieutenant General (Ret.) Michael V. Hayden is the former Director of  
2 the NSA, in office from March 1999 to April 2005. While Director, Defendant Hayden had ultimate  
3 authority for supervising and implementing all operations and functions of the NSA, including the  
4 Program.

5           28.     Defendant United States is the United States of America, its departments, agencies,  
6 and entities.

7           29.     Defendant George W. Bush is the current President of the United States, in office  
8 since January 2001. Mr. Bush authorized and continues to authorize the Program.

9           30.     Defendant Richard B. Cheney is the current Vice President of the United States, in  
10 office since January 2001. Defendant Cheney was personally involved in the creation, development  
11 and implementation of the Program.

12           31.     Defendant David S. Addington is currently the chief of staff to Defendant Cheney,  
13 in office since October 2005. Previously, Defendant Addington served as legal counsel to the Office  
14 of the Vice President. Defendant Addington was personally involved in the creation, development  
15 and implementation of the Program. On information and belief, Defendant Addington drafted the  
16 documents that purportedly authorized the Program.

17           32.     Defendant Department of Justice is a Cabinet-level executive department in the  
18 United States government charged with law enforcement, defending the interests of the United States  
19 according to the law, and ensuring fair and impartial administration of justice for all Americans.

20           33.     Defendant Michael B. Mukasey is the current Attorney General of the United States,  
21 in office since November 2007. As Attorney General, Defendant Mukasey approves and authorizes  
22 the Program on behalf of the Department of Justice.

23           34.     Defendant Alberto R. Gonzales is the former Attorney General of the United States,  
24 in office from February 2005 to September 2007, and also served as White House Counsel to  
25 President George W. Bush from January 2001 to February 2005. Defendant Gonzales was  
26 personally involved in the creation, development and implementation of the Program. As Attorney  
27

1 General, Defendant Gonzales authorized and approved the Program on behalf of the Department of  
2 Justice.

3 35. Defendant John D. Ashcroft is the former Attorney General of the United States, in  
4 office from January 2001 to February 2005. As Attorney General, Defendant Ashcroft authorized  
5 and approved the Program on behalf of the Department of Justice.  
6

7 36. Defendant Vice Admiral (Ret.) John M. McConnell is the Director of National  
8 Intelligence (“DNI”), in office since February 2007. Defendant McConnell has authority over the  
9 activities of the U.S. intelligence community, including the Program.

10 37. Defendant John D. Negroponte was the first Director of National Intelligence, in  
11 office from April 2005 to February 2007. As DNI, Defendant Negroponte had authority over the  
12 activities of the U.S. intelligence community, including the Program.

13 38. At all times relevant hereto, Defendants Doe Nos. 1-100, inclusive (the “Doe  
14 defendants”), whose actual names Plaintiffs have been unable to ascertain notwithstanding  
15 reasonable efforts to do so, but who are sued herein by the fictitious designation “Doe # 1” through  
16 “Doe # 100,” were agents or employees of the NSA, the DOJ, the White House, or were other  
17 government agencies or entities or the agents or employees of such agencies or entities, who  
18 authorized or participated in the Program. Plaintiffs will amend this complaint to allege their true  
19 names and capacities when ascertained. Upon information and belief each fictitiously named  
20 Defendant is responsible in some manner for the occurrences herein alleged and the injuries to  
21 Plaintiffs and class members herein alleged were proximately caused in relation to the conduct of  
22 Does 1-100 as well as the named Defendants.

23 **FACTUAL ALLEGATIONS RELATED TO ALL COUNTS**

24 **THE PRESIDENT’S AUTHORIZATION OF THE PROGRAM**

25 39. On October 4, 2001, President Bush, in concert with White House Counsel Gonzales,  
26 NSA Director Hayden, Attorney General Ashcroft and other Defendants, issued a secret presidential  
27 order (the “Program Order”) authorizing a range of surveillance activities inside of the United States  
28

1 without statutory authorization or court approval, including electronic surveillance of Americans'  
2 telephone and Internet communications (the "Program").

3 40. This Program of surveillance inside the United States began at least by October 6,  
4 2001, and continues to this day.

5 41. The President renewed and, on information and belief, renews his October 4, 2001  
6 order approximately every 45 days.

7 42. The Program of domestic surveillance authorized by the President and conducted by  
8 Defendants required and requires the assistance of major telecommunications companies such as  
9 AT&T, whose cooperation in the Program was and on information and belief is obtained based on  
10 periodic written requests from Defendants and/or other government agents indicating that the  
11 President has authorized the Program's activities, and/or based on oral requests from Defendants  
12 and/or other government agents.

13 43. The periodic written requests issued to colluding telecommunications companies,  
14 including AT&T, have stated and on information and belief do state that the Program's activities  
15 have been determined to be lawful by the Attorney General, except for one period of less than sixty  
16 days.

17 44. On information and belief, at some point prior to March 9, 2004, the Department of  
18 Justice concluded that certain aspects of the Program were in excess of the President's authority and  
19 in violation of criminal law.

20 45. On Tuesday, March 9, 2004, Acting Attorney General James Comey advised the  
21 Administration that he saw no legal basis for certain aspects of the Program. The then-current  
22 Program authorization was set to expire March 11, 2004.

23 46. On Thursday, March 11, 2004, the President renewed the Program Order without a  
24 certification from the Attorney General that the conduct it authorized was lawful.

25 47. On information and belief, the March 11 Program Order instead contained a  
26 statement that the Program's activities had been determined to be lawful by Counsel to the President  
27 Alberto Gonzales, and expressly claimed to override the Department of Justice's conclusion that the  
28

1 Program was unlawful as well as any act of Congress or judicial decision purporting to constrain the  
2 President's power as commander in chief.

3 48. For a period of less than sixty days, beginning on or around March 11, 2004, written  
4 requests to the telecommunications companies asking for cooperation in the Program stated that the  
5 Counsel to the President, rather than the Attorney General, had determined the Program's activities  
6 to be legal.

7 49. By their conduct in authorizing, supervising, and implementing the Program,  
8 Defendants, including the President, the Vice-President, the Attorneys General and the Directors of  
9 NSA since October 2001, the Directors of National Intelligence since 2005 and the Doe defendants,  
10 have aided, abetted, counseled, commanded, induced or procured the commission of all Program  
11 activities herein alleged, and proximately caused all injuries to Plaintiffs herein alleged.

12 **THE NSA'S DRAGNET INTERCEPTION OF COMMUNICATIONS TRANSMITTED**  
13 **THROUGH AT&T FACILITIES**

14 50. AT&T is a provider of electronic communications services, providing to the public  
15 the ability to send or receive wire or electronic communications.

16 51. AT&T is also a provider of remote computing services, providing to the public  
17 computer storage or processing services by means of an electronic communications system.

18 52. Plaintiffs and class members are, or at pertinent times were, subscribers to and/or  
19 customers of AT&T's electronic communications services and/or computer storage or processing  
20 services.

21 53. AT&T maintains domestic telecommunications facilities over which millions of  
22 Americans' telephone and Internet communications pass every day.

23 54. These facilities allow for the transmission of interstate and/or foreign electronic voice  
24 and data communications by the aid of wire, fiber optic cable, or other like connection between the  
25 point of origin and the point of reception.

26 55. One of these AT&T facilities is located at on Folsom Street in San Francisco, CA  
27 (the "Folsom Street Facility").

28



1           56.     The Folsom Street Facility contains a “4ESS Switch Room.” A 4ESS switch is a  
2 type of electronic switching system used to route long-distance telephone communications transiting  
3 through the facility.

4           57.     The Folsom Street Facility also contains a “WorldNet Internet Room” containing  
5 large routers, racks of modems for AT&T customers’ WorldNet dial-up services, and other  
6 telecommunications equipment through which wire and electronic communications to and from  
7 AT&T’s dial-up and DSL Internet service subscribers, including emails, instant messages, Voice-  
8 Over-Internet-Protocol (“VOIP”) conversations and web browsing requests, are transmitted.

9           58.     The communications transmitted through the WorldNet Internet room are carried as  
10 light signals on fiber-optic cables that are connected to routers for AT&T’s WorldNet Internet  
11 service and are a part of AT&T’s Common Backbone Internet network (“CBB”), which comprises  
12 a number of major hub facilities such as the Folsom Street Facility that are connected by a mesh of  
13 high-speed fiber optic cables and that are used for the transmission of interstate and foreign  
14 communications.

15           59.     The WorldNet Internet Room is designed to route and transmit vast amounts of  
16 Internet communications that are “peered” by AT&T between AT&T’s CBB and the networks of  
17 other carriers, such as ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global  
18 Crossing, C&W, UUNET, Level 3, Sprint, Telia, PSINet, and MAE-West. “Peering” is the process  
19 whereby Internet providers interchange traffic destined for their respective customers, and for  
20 customers of their customers.

21           60.     Around January 2003, the NSA designed and implemented a program in  
22 collaboration with AT&T to build a surveillance operation at AT&T’s Folsom Street Facility, inside  
23 a secret room known as the “SG3 Secure Room”.

24           61.     The SG3 Secure Room was built adjacent to the Folsom Street Facility’s 4ESS  
25 switch room.

26           62.     An AT&T employee cleared and approved by the NSA was charged with setting up  
27 and maintaining the equipment in the SG3 Secure Room, and access to the room was likewise  
28 controlled by those NSA-approved AT&T employees.

1           63.     The SG3 Secure Room contains sophisticated computer equipment, including a  
2 device know as aNarus Semantic Traffic Analyzer (the Narus STA”), which is designed to analyze  
3 large volumes of communications at high speed, and can be programmed to analyze the contents and  
4 traffic patterns of communications according to user-defined rules.

5           64.     By early 2003, AT&T—under the instruction and supervision of the NSA—had  
6 connected the fiber-optic cables used to transmit electronic and wire communications through the  
7 WorldNet Internet Room to a “splitter cabinet” that intercepts a copy of all communications  
8 transmitted through the WorldNet Internet Room and diverts copies of those communications to the  
9 equipment in the SG3 Secure Room. (Hereafter, the technical means used to receive the diverted  
10 communications will be referred to as the “Surveillance Configuration.”)

11           65.     The equipment in the SG3 Secure Room is in turn connected to a private high-speed  
12 backbone network separate from the CBB (the “SG3 Network”).

13           66.     NSA analysts communicate instructions to the SG3 Secure Room’s equipment,  
14 including theNarus STA, using the SG3 Network, and the SG3 Secure Room’s equipment transmits  
15 communications based on those rules back to NSA personnel using the SG3 Network.

16           67.     The NSA in cooperation with AT&T has installed and is operating a nationwide  
17 network of Surveillance Configurations in AT&T facilities across the country, connected to the SG3  
18 Network.

19           68.     This network of Surveillance Configurations includes surveillance devices installed  
20 at AT&T facilities in Atlanta, GA; Bridgeton, MO; Los Angeles, CA; San Diego, CA; San Jose CA;  
21 and/or Seattle, WA.

22           69.     Those Surveillance Configurations divert all peered Internet traffic transiting those  
23 facilities into SG3 Secure Rooms connected to the secure SG3 Network used by the NSA, and  
24 information of interest is transmitted from the equipment in the SG3 Secure Rooms to the NSA  
25 based on rules programmed by the NSA.

26           70.     This network of Surveillance Configurations indiscriminately acquires domestic  
27 communications as well as international and foreign communications.

1           71.    This network of Surveillance Configurations involves considerably more locations  
2 than would be required to capture the majority of international traffic.

3           72.    This network of Surveillance Configurations acquires over half of AT&T's purely  
4 domestic Internet traffic, representing almost all of the AT&T traffic to and from other providers,  
5 and comprising approximately 10% of all purely domestic Internet communications in the United  
6 States, including those of non-AT&T customers.

7           73.    Through this network of Surveillance Configurations and/or by other means,  
8 Defendants have acquired and continue to acquire the contents of domestic and international wire  
9 and/or electronic communications sent and/or received by Plaintiffs and class members, as well as  
10 non-content dialing, routing, addressing and/or signaling information pertaining to those  
11 communications.

12           74.    In addition to acquiring all of the Internet communications passing through a number  
13 of key AT&T facilities, Defendants and AT&T acquire all or most long-distance domestic and  
14 international phone calls to or from AT&T long-distance customers, including both the content of  
15 those calls and dialing, routing, addressing and/or signaling information pertaining to those calls,  
16 by using a similarly nationwide network of surveillance devices attached to AT&T's long-distance  
17 telephone switching facilities, and/or by other means.

18           75.    The contents of communications to which Plaintiffs and class members were a party,  
19 and dialing, routing, addressing, and/or signaling information pertaining to those communications,  
20 were and are acquired by Defendants in cooperation with AT&T by using the nationwide network  
21 of Surveillance Configurations, and/or by other means.

22           76.    Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
23 class members' communications contents and non-content information is done without judicial,  
24 statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and  
25 in excess of statutory and constitutional authority.

26           77.    Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs'  
27 and class members' communications contents and non-content information is done without  
28

1 probable cause or reasonable suspicion to believe that Plaintiffs or class members have  
2 committed or are about to commit any crime or engage in any terrorist activity.

3 78. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
4 class members' communications contents and non-content information is done without probable  
5 cause or reasonable suspicion to believe that Plaintiffs or class members are foreign powers or agents  
6 thereof.

7 79. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
8 class members' communications contents and non-content information is done without any reason  
9 to believe that the information is relevant to an authorized criminal investigation or to an authorized  
10 investigation to protect against international terrorism or clandestine intelligence activities.

11 80. Defendants' above-described acquisition in cooperation with AT&T of Plaintiffs' and  
12 class members' communications contents and non-content information was directly performed,  
13 and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

14 81. On information and belief, Defendants will continue to directly acquire, and/or aid,  
15 abet, counsel, command, induce or procure the above-described acquisition in cooperation with  
16 AT&T, the communications contents and non-content information of Plaintiffs and class members.

17 **THE NSA'S DRAGNET COLLECTION OF COMMUNICATIONS RECORDS FROM**  
18 **AT&T DATABASES**

19 82. Defendants have since October 2001 continuously solicited and obtained the  
20 disclosure of all information in AT&T's major databases of stored telephone and Internet records,  
21 including up-to-the-minute updates to the databases that are disclosed in or near real-time.

22 83. Defendants have solicited and obtained from AT&T records concerning  
23 communications to which Plaintiffs and class members were a party, and continue to do so.

24 84. In particular, Defendants have solicited and obtained the disclosure of information  
25 managed by AT&T's "Daytona" database management technology, which includes records  
26 concerning both telephone and Internet communications, and continues to do so.  
27  
28

1           85.     Daytona is a database management technology designed to handle very large  
2 databases and is used to manage "Hawkeye," AT&T's call detail record ("CDR") database, which  
3 contains records of nearly every telephone communication carried over its domestic network since  
4 approximately 2001, records that include the originating and terminating telephone numbers and the  
5 time and length for each call.

6  
7           86.     The Hawkeye CDR database contains records or other information pertaining to  
8 Plaintiffs' and class members' use of AT&T's long distance telephone service and dial-up Internet  
9 service.

10           87.     As of September 2005, all of the CDR data managed by Daytona, when  
11 uncompressed, totaled more than 312 terabytes.

12           88.     Daytona is also used to manage AT&T's huge network-security databasc, known as  
13 "Aurora," which has been used to store Internet traffic data since approximately 2003. The Aurora  
14 database contains huge amounts of data acquired by firewalls, routershoneypots and other devices  
15 on AT&T's global IP (Internet Protocol) network and other networks connected to AT&T's network.

16  
17           89.     The Aurora databasc managed by Daytona contains records or other information  
18 pertaining to Plaintiffs' and class members' use of AT&T's Internet services.

19           90.     Since October 6, 2001 or shortly thereafter, Defendants have continually solicited  
20 and obtained from AT&T disclosure of the contents of the Hawkeye and Aurora communications  
21 records databases and/or other AT&T communications records, including records or other  
22 information pertaining to Plaintiffs' and class members' use of AT&T's telephone and Internet  
23 services.

24           91.     The NSA and/or other Defendants maintain the communications records disclosed  
25 by AT&T in their own database or databases of such records.

26  
27           92.     Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
28 and class members' communications records, and its receipt of such disclosure, is done without

1 judicial, statutory, or other lawful authorization, in violation of statutory and constitutional  
2 limitations, and in excess of statutory and constitutional authority.

3 93. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
4 and class members' communications records, and its receipt of such disclosure, is done without  
5 probable cause or reasonable suspicion to believe that Plaintiffs' or class members have  
6 committed or are about to commit any crime or engage in any terrorist activity.

7  
8 94. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
9 and class members' communications records, and its receipt of such disclosure, is done without  
10 probable cause or reasonable suspicion to believe that Plaintiffs' or class members are foreign  
11 powers or agents thereof.

12 95. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
13 and class members' communications records, and its receipt of such disclosure, is done without any  
14 reason to believe that the information is relevant to an authorized criminal investigation or to an  
15 authorized investigation to protect against international terrorism or clandestine intelligence  
16 activities.

17 96. Defendants' above-described solicitation of the disclosure by AT&T of Plaintiffs'  
18 and class members' communications records, and its receipt of such disclosure, is directly  
19 performed, and/or aided, abetted, counseled, commanded, induced or procured, by Defendants.

20 97. On information and belief, Defendants will continue to directly solicit and obtain  
21 AT&T's disclosure of its communications records, including records pertaining to Plaintiffs and  
22 class members, and/or will continue to aid, abet, counsel, command, induce or procure that conduct.

23 **CLASS ACTION ALLEGATIONS**

24 98. Pursuant to Federal Rules of Civil Procedure, Rule 23(b)(2), Plaintiffs Hepting,  
25 Hicks, Jewel, Knutzen, and Walton bring this action on behalf of themselves and a class of similarly  
26 situated persons defined as:  
27

28

1 All individuals in the United States that are current residential subscribers or  
2 customers of AT&T's telephone services or Internet services, or that were residential  
telephone or Internet subscribers or customers at any time after September 2001.

3 99. The class seeks certification of claims for declaratory, injunctive and other equitable  
4 relief pursuant to 18 U.S.C. §2520, 18 U.S.C. §2707 and 5 U.S.C. § 702, in addition to declaratory  
5 and injunctive relief for violations of the First and Fourth Amendments. Members of the class  
6 expressly and personally retain any and all damages claims they individually may possess arising  
7 out of or relating to the acts, events, and transactions that form the basis of this action. The  
8 individual damages claims of the class members are outside the scope of this class action.  
9

10 100. Excluded from the class are the individual Defendants, all who have acted in active  
11 concert and participation with the individual Defendants, and the legal representatives, heirs,  
12 successors, and assigns of the individual Defendants.

13 101. Also excluded from the class are any foreign powers, as defined by 50 U.S.C.  
14 § 1801(a), or any agents of foreign powers, as defined by 50 U.S.C. § 1801(b)(1)(A), including  
15 without limitation anyone who knowingly engages in sabotage or international terrorism, or  
16 activities that are in preparation therefore.  
17

18 102. This action is brought as a class action and may properly be so maintained pursuant  
19 to the provisions of the Federal Rules of Civil Procedure, Rule 23. Plaintiffs reserve the right to  
20 modify the class definition and the class period based on the results of discovery.

21 103. **Numerosity of the Class:** Members of the class are so numerous that their  
22 individual joinder is impracticable. The precise numbers and addresses of members of the class are  
23 unknown to the Plaintiffs. Plaintiffs estimate that the class consists of millions of members. The  
24 precise number of persons in the class and their identities and addresses may be ascertained from  
25 Defendants' and AT&T's records.  
26  
27  
28

1           104. **Existence of Common Questions of Fact and Law**: There is a well-defined  
2 community of interest in the questions of law and fact involved affecting the members of the class.

3 These common legal and factual questions include:

4           (a) Whether Defendants have violated the First and Fourth Amendment rights of  
5 class members, or are currently doing so;

6           (b) Whether Defendants have subjected class members to electronic surveillance,  
7 or have disclosed or used information obtained by electronic surveillance of the class members, in  
8 violation of 50 U.S.C. § 1809, or are currently doing so;

9           (c) Whether Defendants have intercepted, used or disclosed class members'  
10 communications in violation of 18 U.S.C. § 2511, or are currently doing so;

11           (d) Whether Defendants have solicited and obtained the disclosure of the  
12 contents of class members' communications in violation of 18 U.S.C. § 2703(a) or (b), or are  
13 currently doing so;

14           (e) Whether Defendants have solicited or obtained the disclosure of non-content  
15 records or other information pertaining to class members in violation of 18 U.S.C. § 2703(c), or are  
16 currently doing so;

17           (f) Whether Defendants have violated the Administrative Procedures Act, 5  
18 U.S.C. §§ 701 *et seq.*, or are currently doing so;

19           (g) Whether the Defendants have violated the constitutional principle of  
20 separation of powers, or are currently doing so;

21           (h) Whether Plaintiffs and class members are entitled to injunctive, declaratory,  
22 and other equitable relief against Defendants;

23           (i) Whether Plaintiffs and class members are entitled to an award of reasonable  
24 attorneys' fees and costs of this suit.

25           105. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the class  
26 because Plaintiffs are or were subscribers to the Internet and telephone services of Defendants.  
27  
28





1 of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of  
2 Plaintiffs' and class members' communications, contents of communications, and records pertaining  
3 to their communications transmitted, collected, and/or stored by AT&T, without judicial or other  
4 lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and  
5 constitutional limitations, and in excess of statutory and constitutional authority.  
6

7 111. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
8 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition,  
9 interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications,  
10 contents of communications, and records pertaining to their communications transmitted, collected,  
11 and/or stored by AT&T, without judicial or other lawful authorization, probable cause, and/or  
12 individualized suspicion.  
13

14 112. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the  
15 above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs and class  
16 members by obtaining judicial or other lawful authorization and by conforming their conduct to the  
17 requirements of the Fourth Amendment.  
18

19 113. By the acts alleged herein, Defendants have violated Plaintiffs' and class members'  
20 reasonable expectations of privacy and denied Plaintiffs and class members their right to be free  
21 from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution  
22 of the United States.  
23

24 114. By the acts alleged herein, Defendants' conduct has proximately caused harm to  
25 Plaintiffs and class members.  
26

27 115. Defendants' conduct was done intentionally, with deliberate indifference, or with  
28 reckless disregard of, Plaintiffs' and class members' constitutional rights.



1 of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of  
2 Plaintiffs' communications, contents of communications, and records pertaining to their  
3 communications transmitted, collected, and/or stored by AT&T without judicial or other lawful  
4 authorization, probable cause, and/or individualized suspicion, in violation of statutory and  
5 constitutional limitations, and in excess of statutory and constitutional authority.  
6

7 121. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
8 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition,  
9 interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of  
10 communications, and records pertaining to their communications transmitted, collected, and/or  
11 stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized  
12 suspicion.  
13

14 122. At all relevant times, Defendants committed, knew of and/or acquiesced in all of the  
15 above-described acts, and failed to respect the Fourth Amendment rights of Plaintiffs by obtaining  
16 judicial or other lawful authorization and conforming their conduct to the requirements of the Fourth  
17 Amendment.  
18

19 123. By the acts alleged herein, Defendants have violated Plaintiffs' reasonable  
20 expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and  
21 seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.  
22

23 124. By the acts alleged herein, Defendants' conduct has proximately caused harm to  
24 Plaintiffs.  
25

26 125. Defendants' conduct was done intentionally, with deliberate indifference, or with  
27 reckless disregard of, Plaintiffs' constitutional rights.  
28

126. Plaintiffs seek an award of their actual damages and punitive damages against the  
Count II Defendants, and such other or further relief as is proper.

**COUNT III**

**Violation of First Amendment—Declaratory, Injunctive, and Other Equitable Relief**

**(Named Plaintiffs and Class vs. Defendants United States, National Security Agency, Department of Justice, Bush (in his official and personal capacities), Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)**

127. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

128. Plaintiffs and class members use AT&T's services to speak or receive speech anonymously and to associate privately.

129. Defendants directly performed, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' and class members' communications, contents of communications, and records pertaining to their communications without judicial or other lawful authorization, probable cause, and/or individualized suspicion, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.

130. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition, interception, disclosure, divulgence and/or use of Plaintiffs' communications, contents of communications, and records pertaining to their communications transmitted, collected, and/or stored by AT&T without judicial or other lawful authorization, probable cause, and/or individualized suspicion.

131. By the acts alleged herein, Defendants violated Plaintiffs' and class members' rights to speak and to receive speech anonymously and associate privately under the First Amendment.





1 except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or  
2 any express statutory authorization that is an additional exclusive means for  
3 conducting electronic surveillance under section 1812 of this title; or (2)  
4 discloses or uses information obtained under color of law by electronic  
5 surveillance, knowing or having reason to know that the information was  
6 obtained through electronic surveillance not authorized by this chapter,  
7 chapter 119, 121, or 206 of Title 18 or any express statutory authorization  
8 that is an additional exclusive means for conducting electronic surveillance  
9 under section 1812 of this title.

10 145. In relevant part 50 U.S.C. § 1801 provides that:

11 (f) "Electronic surveillance" means – (1) the acquisition by an electronic,  
12 mechanical, or other surveillance device of the contents of any wire or radio  
13 communication sent by or intended to be received by a particular, known  
14 United States person who is in the United States, if the contents are acquired  
15 by intentionally targeting that United States person, under circumstances in  
16 which a person has a reasonable expectation of privacy and a warrant would  
17 be required for law enforcement purposes; (2) the acquisition by an  
18 electronic, mechanical, or other surveillance device of the contents of any  
19 wire communication to or from a person in the United States, without the  
20 consent of any party thereto, if such acquisition occurs in the United States,  
21 but does not include the acquisition of those communications of computer  
22 trespassers that would be permissible under section 2511(2)(i) of Title 18; (3)  
23 the intentional acquisition by an electronic, mechanical, or other surveillance  
24 device of the contents of any radio communication, under circumstances in  
25 which a person has a reasonable expectation of privacy and a warrant would  
26 be required for law enforcement purposes, and if both the sender and all  
27 intended recipients are located within the United States; or (4) the installation  
28 or use of an electronic, mechanical, or other surveillance device in the United  
States for monitoring to acquire information, other than from a wire or radio  
communication, under circumstances in which a person has a reasonable  
expectation of privacy and a warrant would be required for law enforcement  
purposes.

146. 18 U.S.C. § 2511(2)(f) further provides in relevant part that "procedures in this  
chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive*  
*means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act,  
and the interception of domestic wire, oral, and electronic communications may be conducted."

(Emphasis added.)

147. 50 U.S.C. § 1812 further provides in relevant part that:

(a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
and 206 of Title 18 and this chapter shall be the *exclusive means* by which



1 electronic surveillance and the interception of domestic wire, oral, or  
2 electronic communications may be conducted.

3 (b) Only an express statutory authorization for electronic surveillance or the  
4 interception of domestic wire, oral, or electronic communications, other than  
as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
constitute an additional exclusive means for the purpose of subsection (a).

5 (Emphasis added.)

6 148. Defendants intentionally acquired, or aided, abetted, counseled, commanded,  
7 induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in,  
8 enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission  
9 of such acquisition, by means of a surveillance device, the contents of one or more wire  
10 communications to or from Plaintiffs and class members or other information in which Plaintiffs or  
11 class members have a reasonable expectation of privacy, without the consent of any party thereto,  
12 and such acquisition occurred in the United States.

14 149. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
15 contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition  
16 of Plaintiffs' communications.

17 150. By the acts alleged herein, Defendants acting in excess of their statutory authority  
18 and in violation of statutory limitations have intentionally engaged in, or aided, abetted, counseled,  
19 commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused,  
20 participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in  
21 the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under color of law,  
22 not authorized by any statute, to which Plaintiffs and class members were subjected in violation of  
23 50 U.S.C. § 1809.

24 151. Additionally or in the alternative, by the acts alleged herein, Defendants acting in  
25 excess of their statutory authority and in violation of statutory limitations have intentionally  
26 disclosed or used information obtained under color of law by electronic surveillance, knowing or  
27  
28

1 having reason to know that the information was obtained through electronic surveillance not  
2 authorized by statute, including information pertaining to Plaintiffs and class members, or aided,  
3 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
4 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
5 or conspired in the commission of such acts.

6  
7 152. Defendants did not notify Plaintiffs or class members of the above-described  
8 electronic surveillance, disclosure, and/or use, nor did Plaintiffs or class members consent to such.

9 153. Plaintiffs and class members have been and are aggrieved by Defendants' electronic  
10 surveillance, disclosure, and/or use of their wire communications.

11 154. On information and belief, the Count V Defendants are now engaging in and will  
12 continue to engage in the above-described acts resulting in the electronic surveillance, disclosure,  
13 and/or use of Plaintiffs' and class members' wire communications, acting in excess of the Count V  
14 Defendants' statutory authority and in violation of statutory limitations, including 50 U.S.C. § 1809  
15 and 18 U.S.C. § 2511(2)(f), and are thereby irreparably harming Plaintiffs and class members.  
16 Plaintiffs and class members have no adequate remedy at law for the Count V Defendants'  
17 continuing unlawful conduct, and the Count V Defendants will continue to violate Plaintiffs' and  
18 class members' legal rights unless enjoined and restrained by this Court.

19  
20 155. Pursuant to *Larson v. United States*, 337 U.S. 682 (1949) and to 5 U.S.C. § 702,  
21 Plaintiffs seek that this Court declare that Defendants have violated their rights and the rights of the  
22 class; enjoin the Count V Defendants, their agents, successors, and assigns, and all those in active  
23 concert and participation with them from violating the Plaintiffs' and class members' statutory  
24 rights, including their rights under 50 U.S.C. §§ 1801 *et seq.*; and award such other and further  
25 equitable relief as is proper.  
26  
27  
28

**COUNT VI**

**Violation of 50 U.S.C. § 1809, actionable under 50 U.S.C. § 1810—Damages**

**(Named Plaintiffs vs. Defendants United States, National Security Agency, Department of Justice, Alexander (in his official and personal capacities), Hayden (in his personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity), Mukasey (in his official and personal capacities), Gonzales (in his personal capacity), Ashcroft (in his personal capacity), McConnell (in his official and personal capacities), and Negroponte (in his personal capacity), and one or more of the Doe Defendants)**

156. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

157. In relevant part, 50 U.S.C. § 1809 provides that:

(a) Prohibited activities—A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by this chapter, chapter 119, 121, or 206 of Title 18 or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 1812 of this title.

158. In relevant part 50 U.S.C. § 1801 provides that:

(f) “Electronic surveillance” means – (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18; (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

159. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.”

(Emphasis added.)

160. 50 U.S.C. § 1812 further provides in relevant part that:

(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of Title 18 and this chapter shall be the *exclusive means* by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall constitute an additional exclusive means for the purpose of subsection (a).

(Emphasis added.)

161. Defendants intentionally acquired, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the commission of such acquisition, by means of a surveillance device, the contents of one or more wire communications to or from Plaintiffs or other information in which Plaintiffs have a reasonable expectation of privacy, without the consent of any party thereto, and such acquisition occurred in the United States.

162. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of the above-described acts of acquisition of Plaintiffs’ communications.

1           163. By the acts alleged herein, Defendants have intentionally engaged in, or aided,  
2 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
3 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
4 or conspired in the commission of, electronic surveillance (as defined by 50 U.S.C. § 1801(f)) under  
5 color of law, not authorized by any statute, to which Plaintiffs were subjected in violation of 50  
6 U.S.C. § 1809.  
7

8           164. Additionally or in the alternative, by the acts alleged herein, Defendants have  
9 intentionally disclosed or used information obtained under color of law by electronic surveillance,  
10 knowing or having reason to know that the information was obtained through electronic surveillance  
11 not authorized by statute, including information pertaining to Plaintiffs, or aided, abetted, counseled,  
12 commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused,  
13 participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in  
14 the commission of such acts.  
15

16           165. Defendants did not notify Plaintiffs of the above-described electronic surveillance,  
17 disclosure, and/or use, nor did Plaintiffs consent to such.  
18

19           166. Plaintiffs have been and are aggrieved by Defendants' electronic surveillance,  
20 disclosure, and/or use of their wire communications.  
21

22           167. Pursuant to 50 U.S.C. § 1810, which provides a civil action for any person who has  
23 been subjected to an electronic surveillance or about whom information obtained by electronic  
24 surveillance of such person has been disclosed or used in violation of 50 U.S.C. § 1809, Plaintiffs  
25 seek from the Court VI Defendants for each Plaintiff their statutory damages or actual damages;  
26 punitive damages as appropriate; and such other and further relief as is proper.  
27  
28

**COUNT VII**

**Violation of 18 U.S.C. § 2511—Declaratory, Injunctive, and Other Equitable Relief**

**(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal capacities), Mukasey (in his official and personal capacities), and McConnell (in his official and personal capacities), and one or more of the Doe Defendants)**

168. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

169. In relevant part, 18 U.S.C. § 2511 provides that:

(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

170. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

171. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.” (Emphasis added.)

172. 50 U.S.C. § 1812 further provides in relevant part that:

1 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
2 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
3 electronic surveillance and the interception of domestic wire, oral, or  
4 electronic communications may be conducted.

5 (b) Only an express statutory authorization for electronic surveillance or the  
6 interception of domestic wire, oral, or electronic communications, other than  
7 as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
8 constitute an additional exclusive means for the purpose of subsection (a).

9 (Emphasis added.)

10 173. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
11 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs'  
12 and class members' wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

13 174. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
14 endeavored to disclose, to another person the contents of Plaintiffs' and class members' wire or  
15 electronic communications, knowing or having reason to know that the information was obtained  
16 through the interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c);  
17 and/or

18 175. By the acts alleged herein, Defendants have intentionally and willfully used, or  
19 endeavored to use, the contents of Plaintiffs' and class members' wire or electronic communications,  
20 while knowing or having reason to know that the information was obtained through the interception  
21 of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(d).

22 176. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
23 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
24 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
25 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
26 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

27 177. Defendants have committed these acts of interception, disclosure, divulgence and/or  
28 use of Plaintiffs' and class members' communications directly or by aiding, abetting, counseling,

1 commanding, inducing, procuring, encouraging, promoting, instigating, advising, willfully causing  
2 participating in, enabling, contributing to, facilitating, directing, controlling, assisting in, or  
3 conspiring in their commission. In doing so, Defendants have acted in excess of their statutory  
4 authority and in violation of statutory limitations.

5  
6 178. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
7 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
8 divulgence and/or use of Plaintiffs' and class members' communications.

9 179. Defendants did not notify Plaintiffs or class members of the above-described  
10 intentional interception, disclosure, divulgence and/or use of their wire or electronic  
11 communications, nor did Plaintiffs or class members consent to such.

12 180. Plaintiffs and class members have been and are aggrieved by Defendants' intentional  
13 and willful interception, disclosure, divulgence and/or use of their wire or electronic  
14 communications.

15  
16 181. On information and belief, the Count VII Defendants are now engaging in and will  
17 continue to engage in the above-described acts resulting in the intentional and willful interception,  
18 disclosure, divulgence and/or use of Plaintiffs' and class members' wire or electronic  
19 communications, acting in excess of the Count VII Defendants' statutory authority and in violation  
20 of statutory limitations, including 18 U.S.C. § 2511, and are thereby irreparably harming Plaintiffs  
21 and class members. Plaintiffs and class members have no adequate remedy at law for the Count VII  
22 Defendants' continuing unlawful conduct, and the Count VII Defendants will continue to violate  
23 Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

24  
25 182. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose  
26 wire or electronic communications have been intercepted, disclosed, divulged or intentionally used  
27 in violation of 18 U.S.C. § 2511, to *Larson v. United States*, 337 U.S. 682 (1949), and to 5 U.S.C.  
28



1 § 702, Plaintiffs and class members seek equitable and declaratory relief against the Count VII  
2 Defendants.

3 183. Plaintiffs seek that this Court declare that Defendants have violated their rights and  
4 the rights of the class; enjoin the Count VII Defendants, their agents, successors, and assigns, and  
5 all those in active concert and participation with them from violating the Plaintiffs' and class  
6 members' statutory rights, including their rights under 18 U.S.C. § 2511; and award such other and  
7 further equitable relief as is proper.  
8

9 **COUNT VIII**

10 **Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2520—Damages**

11 **(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his**  
12 **personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity),**  
13 **Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his**  
14 **personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal**  
15 **capacity), and one or more of the Doe Defendants)**

16 184. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
17 paragraphs of this complaint, as if set forth fully herein.

18 185. In relevant part, 18 U.S.C. § 2511 provides that:

19 (1) Except as otherwise specifically provided in this chapter any person who  
20 – (a) intentionally intercepts, endeavors to intercept, or procures any other  
21 person to intercept or endeavor to intercept, any wire, oral, or electronic  
22 communication . . . (c) intentionally discloses, or endeavors to disclose, to  
23 any other person the contents of any wire, oral, or electronic communication,  
24 knowing or having reason to know that the information was obtained through  
25 the interception of a wire, oral, or electronic communication in violation of  
26 this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents  
27 of any wire, oral, or electronic communication, knowing or having reason to  
28 know that the information was obtained through the interception of a wire,  
oral, or electronic communication in violation of this subsection . . . shall be  
punished as provided in subsection (4) or shall be subject to suit as provided  
in subsection (5).

186. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or  
entity providing an electronic communication service to the public shall not  
intentionally divulge the contents of any communication (other than one to

1 such person or entity, or an agent thereof) while in transmission on that  
2 service to any person or entity other than an addressee or intended recipient  
of such communication or an agent of such addressee or intended recipient.

3 187. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this  
4 chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive*  
5 *means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act,  
6 and the interception of domestic wire, oral, and electronic communications may be conducted.”

7  
8 (Emphasis added.)

9 188. 50 U.S.C. § 1812 further provides in relevant part that:

10 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
11 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
12 electronic surveillance and the interception of domestic wire, oral, or  
electronic communications may be conducted.

13 (b) Only an express statutory authorization for electronic surveillance or the  
14 interception of domestic wire, oral, or electronic communications, other than  
as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
constitute an additional exclusive means for the purpose of subsection (a).

15 (Emphasis added.)

16 189. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
17 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs’  
18 wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

19 190. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
20 endeavored to disclose, to another person the contents of Plaintiffs’ wire or electronic  
21 communications, knowing or having reason to know that the information was obtained through the  
22 interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

23 191. By the acts alleged herein, Defendants have intentionally and willfully used, or  
24 endeavored to use, the contents of Plaintiffs’ wire or electronic communications, while knowing or  
25 having reason to know that the information was obtained through the interception of wire or  
26 electronic communications in violation of 18 U.S.C. § 2511(1)(d).  
27  
28

1           192. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
2 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
3 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
4 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
5 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).  
6

7           193. Defendants have committed these acts of interception, disclosure, divulgence and/or  
8 use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing,  
9 procuring, encouraging, promoting, instigating, advising, willfully causing, participating in,  
10 enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their  
11 commission.  
12

13           194. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
14 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
15 divulgence and/or use of Plaintiffs' communications.  
16

17           195. Defendants did not notify Plaintiffs of the above-described intentional interception,  
18 disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or  
19 class members consent to such.  
20

21           196. Plaintiffs have been and are aggrieved by Defendants' intentional and willful  
22 interception, disclosure, divulgence and/or use of their wire or electronic communications.  
23

24           197. Pursuant to 18 U.S.C. § 2520, which provides a civil action for any person whose  
25 wire or electronic communications have been intercepted, disclosed, divulged or intentionally used  
26 in violation of 18 U.S.C. § 2511, Plaintiffs seek from the Court VIII Defendants for each Plaintiff  
27 their statutory damages or actual damages; punitive damages as appropriate; and such other and  
28 further relief as is proper.

**COUNT IX**

**Violation of 18 U.S.C. § 2511, actionable under 18 U.S.C. § 2712—Damages Against The United States**

**(Named Plaintiffs vs. Defendants United States, Department of Justice, and National Security Agency)**

198. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

199. In relevant part, 18 U.S.C. § 2511 provides that:

(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . [or](d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

200. 18 U.S.C. § 2511 further provides that:

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

201. 18 U.S.C. § 2511(2)(f) further provides in relevant part that “procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 [50 U.S.C. § 1801] of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.” (Emphasis added.)

202. 50 U.S.C. § 1812 further provides in relevant part that:

1 (a) Except as provided in subsection (b), the procedures of chapters 119, 121,  
2 and 206 of Title 18 and this chapter shall be the *exclusive means* by which  
3 electronic surveillance and the interception of domestic wire, oral, or  
4 electronic communications may be conducted.

5 (b) Only an express statutory authorization for electronic surveillance or the  
6 interception of domestic wire, oral, or electronic communications, other than  
7 as an amendment to this chapter or chapters 119, 121, or 206 of Title 18 shall  
8 constitute an additional exclusive means for the purpose of subsection (a).

9 (Emphasis added.)

10 203. By the acts alleged herein, Defendants have intentionally and willfully intercepted,  
11 endeavored to intercept, or procured another person to intercept or endeavor to intercept, Plaintiffs'  
12 wire or electronic communications in violation of 18 U.S.C. § 2511(1)(a); and/or

13 204. By the acts alleged herein, Defendants have intentionally and willfully disclosed, or  
14 endeavored to disclose, to another person the contents of Plaintiffs' wire or electronic  
15 communications, knowing or having reason to know that the information was obtained through the  
16 interception of wire or electronic communications in violation of 18 U.S.C. § 2511(1)(c); and/or

17 205. By the acts alleged herein, Defendants have intentionally and willfully used, or  
18 endeavored to use, the contents of Plaintiffs' wire or electronic communications, while knowing or  
19 having reason to know that the information was obtained through the interception of wire or  
20 electronic communications in violation of 18 U.S.C. § 2511(1)(d).

21 206. By the acts alleged herein, Defendants have intentionally and willfully caused, or  
22 aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated,  
23 advised, participated in, contributed to, facilitated, directed, controlled, assisted in, or conspired to  
24 cause AT&T's divulgence of Plaintiffs' and class members' wire or electronic communications to  
25 Defendants while in transmission by AT&T, in violation of 18 U.S.C. § 2511(3)(a).

26 207. Defendants have committed these acts of interception, disclosure, divulgence and/or  
27 use of Plaintiffs' communications directly or by aiding, abetting, counseling, commanding, inducing,  
28 procuring, encouraging, promoting, instigating, advising, willfully causing, participating in,

1 enabling, contributing to, facilitating, directing, controlling, assisting in, or conspiring in their  
2 commission.

3 208. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
4 contributing to, facilitating, or assisting in the commission of these acts of interception, disclosure,  
5 divulgence and/or use of Plaintiffs' communications.  
6

7 209. Defendants did not notify Plaintiffs of the above-described intentional interception,  
8 disclosure, divulgence and/or use of their wire or electronic communications, nor did Plaintiffs or  
9 class members consent to such.

10 210. Plaintiffs have been and are aggrieved by Defendants' intentional and willful  
11 interception, disclosure, divulgence and/or use of their wire or electronic communications.  
12

13 211. Title 18 U.S.C. § 2712 provides a civil action against the United States and its  
14 agencies and departments for any person whose wire or electronic communications have been  
15 intercepted, disclosed, divulged or intentionally used in willful violation of 18 U.S.C. § 2511.  
16 Plaintiffs have complied fully with the claim presentment procedure of 18 U.S.C. § 2712. Pursuant  
17 to 18 U.S.C. § 2712, Plaintiffs seek from the Court IX Defendants for each Plaintiff their statutory  
18 damages or actual damages, and such other and further relief as is proper.  
19

20 **COUNT X**

21 **Violation of 18 U.S.C. § 2703(a) & (b)—Declaratory, Injunctive, and Other Equitable  
Relief**

22 **(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal  
23 capacities), Mukasey (in his official and personal capacities), and McConnell (in his official  
and personal capacities), and one or more of the Doe Defendants)**

24 212. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
25 paragraphs of this complaint, as if set forth fully herein.  
26

27 213. In relevant part, 18 U.S.C. § 2703 provides that:  
28

1 (a) Contents of Wire or Electronic Communications in Electronic Storage.— A  
2 governmental entity may require the disclosure by a provider of electronic  
3 communication service of the contents of a wire or electronic communication, that  
4 is in electronic storage in an electronic communications system for one hundred  
5 and eighty days or less, only pursuant to a warrant issued using the procedures  
6 described in the Federal Rules of Criminal Procedure by a court with jurisdiction  
7 over the offense under investigation or equivalent State warrant. A governmental  
8 entity may require the disclosure by a provider of electronic communications  
9 services of the contents of a wire or electronic communication that has been in  
10 electronic storage in an electronic communications system for more than one  
11 hundred and eighty days by the means available under subsection (b) of this  
12 section.

13 (b) Contents of Wire or Electronic Communications in a Remote Computing  
14 Service.—

15 (1) A governmental entity may require a provider of remote computing  
16 service to disclose the contents of any wire or electronic communication to  
17 which this paragraph is made applicable by paragraph (2) of this subsection—

18 (A) without required notice to the subscriber or customer, if the  
19 governmental entity obtains a warrant issued using the procedures  
20 described in the Federal Rules of Criminal Procedure by a court with  
21 jurisdiction over the offense under investigation or equivalent State  
22 warrant; or

23 (B) with prior notice from the governmental entity to the subscriber or  
24 customer if the governmental entity—

25 (i) uses an administrative subpoena authorized by a Federal or State  
26 statute or a Federal or State grand jury or trial subpoena; or

27 (ii) obtains a court order for such disclosure under subsection (d) of this  
28 section;

except that delayed notice may be given pursuant to section 2705 of this  
title.

(2) Paragraph (1) is applicable with respect to any wire or electronic  
communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from  
(or created by means of computer processing of communications received  
by means of electronic transmission from), a subscriber or customer of  
such remote computing service; and

(B) solely for the purpose of providing storage or computer processing  
services to such subscriber or customer, if the provider is not authorized to  
access the contents of any such communications for purposes of providing  
any services other than storage or computer processing.

214. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
abettted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
or conspired in soliciting and obtaining from AT&T, the disclosure to Defendants of the contents

1 of Plaintiffs' and class members' communications while in electronic storage by an AT&T electronic  
2 communication service, and/or while carried or maintained by an AT&T remote computing service,  
3 in violation of 18 U.S.C. §§ 2703(a) and/or (b). In doing so, Defendants have acted in excess of  
4 their statutory authority and in violation of statutory limitations.

5  
6 215. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
7 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
8 and class members' communications.

9 216. Defendants did not notify Plaintiffs or class members of the disclosure of their  
10 communications, nor did Plaintiffs or class members consent to such.

11 217. Plaintiffs and class members have been and are aggrieved by Defendants' above-  
12 described soliciting and obtaining of disclosure of the contents of communications.

13  
14 218. On information and belief, the Count X Defendants are now engaging in and will  
15 continue to engage in the above-described soliciting and obtaining of disclosure of the contents of  
16 class members' communications while in electronic storage by AT&T's electronic communication  
17 service(s), and/or while carried or maintained by AT&T's remote computing service(s), acting in  
18 excess of the Count X Defendants' statutory authority and in violation of statutory limitations,  
19 including 18 U.S.C. § 2703(a) and (b), and are thereby irreparably harming Plaintiffs and class  
20 members. Plaintiffs and class members have no adequate remedy at law for the Count X  
21 Defendants' continuing unlawful conduct, and the Count X Defendants will continue to violate  
22 Plaintiffs' and class members' legal rights unless enjoined and restrained by this Court.

23  
24 219. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved  
25 by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682  
26 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief  
27 against the Count X Defendants.  
28





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

223. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of the contents of Plaintiffs' communications while in electronic storage by an AT&T electronic communication service, and/or while carried or maintained by an AT&T remote computing service, in violation of 18 U.S.C. §§ 2703(a) and/or (b).

224. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' communications.

225. Defendants did not notify Plaintiffs of the disclosure of their communications, nor did Plaintiffs consent to such.

226. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and obtaining of disclosure of the contents of communications.



- 1 (ii) obtains a court order for such disclosure under subsection (d) of  
2 this section;  
3 except that delayed notice may be given pursuant to section 2705 of this  
4 title.  
5 (2) Paragraph (1) is applicable with respect to any wire or electronic  
6 communication that is held or maintained on that service—  
7 (A) on behalf of, and received by means of electronic transmission from  
8 (or created by means of computer processing of communications received  
9 by means of electronic transmission from), a subscriber or customer of  
10 such remote computing service; and  
11 (B) solely for the purpose of providing storage or computer processing  
12 services to such subscriber or customer, if the provider is not authorized to  
13 access the contents of any such communications for purposes of providing  
14 any services other than storage or computer processing.

15 230. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
16 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
17 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
18 or conspired in the soliciting and obtaining from AT&T the disclosure to the NSA of the contents  
19 of Plaintiffs' communications while in electronic storage by an AT&T electronic communication  
20 service, and/or while carried or maintained by an AT&T remote computing service, in violation of  
21 18 U.S.C. §§ 2703(a) and/or (b).

22 231. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
23 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
24 communications.

25 232. Defendants did not notify Plaintiffs of the disclosure of their communications, nor  
26 did Plaintiffs consent to such.

27 233. Plaintiffs have been and are aggrieved by Defendants' above-described soliciting and  
28 obtaining of disclosure of the contents of communications.

29 234. Title 18 U.S.C. § 2712 provides a civil action against the United States and its  
30 agencies and departments for any person whose communications have been disclosed in willful

1 violation of 18 U.S.C. § 2703. Plaintiffs have complied fully with the claim presentment procedure  
2 of 18 U.S.C. § 2712. Pursuant to 18 U.S.C. § 2712, Plaintiffs seek from the Court XII Defendants  
3 for each Plaintiff their statutory damages or actual damages, and such other and further relief as is  
4 proper.

5  
6 **COUNT XIII**

7 **Violation of 18 U.S.C. § 2703(c)—Declaratory, Injunctive, and Other Equitable Relief**

8 **(Named Plaintiffs and Class vs. Defendants Alexander (in his official and personal**  
9 **capacities), Mukasey (in his official and personal capacities), and McConnell (in his official**  
10 **and personal capacities), and one or more of the Doe Defendants)**

11 235. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
12 paragraphs of this complaint, as if set forth fully herein.

13 236. In relevant part, 18 U.S.C. § 2703(c) provides that:

14 **(c) Records Concerning Electronic Communication Service or Remote  
15 Computing Service.—**

16 **(1) A governmental entity may require a provider of electronic  
17 communication service or remote computing service to disclose a record or  
18 other information pertaining to a subscriber to or customer of such service  
19 (not including the contents of communications) only when the governmental  
20 entity—**

21 **(A) obtains a warrant issued using the procedures described in the Federal  
22 Rules of Criminal Procedure by a court with jurisdiction over the offense  
23 under investigation or equivalent State warrant;**

24 **(B) obtains a court order for such disclosure under subsection (d) of this  
25 section;**

26 **(C) has the consent of the subscriber or customer to such disclosure;**

27 **(D) submits a formal written request relevant to a law enforcement  
28 investigation concerning telemarketing fraud for the name, address, and  
place of business of a subscriber or customer of such provider, which  
subscriber or customer is engaged in telemarketing (as such term is  
defined in section 2325 of this title); or**

**(E) seeks information under paragraph (2).**

**(2) A provider of electronic communication service or remote computing  
service shall disclose to a governmental entity the—**

**(A) name;**

**(B) address;**

**(C) local and long distance telephone connection records, or records of  
session times and durations;**

**(D) length of service (including start date) and types of service utilized;**

1 (E) telephone or instrument number or other subscriber number or  
2 identity, including any temporarily assigned network address; and  
3 (F) means and source of payment for such service (including any credit  
4 card or bank account number),  
5 of a subscriber to or customer of such service when the governmental entity  
6 uses an administrative subpoena authorized by a Federal or State statute or a  
7 Federal or State grand jury or trial subpoena or any means available under  
8 paragraph (1).  
9 (3) A governmental entity receiving records or information under this  
10 subsection is not required to provide notice to a subscriber or customer.

11 237. Defendants intentionally and willfully solicited and obtained from AT&T, or aided,  
12 abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised,  
13 willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in,  
14 or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or  
15 other information pertaining to Plaintiffs' and class members' use of electronic communication  
16 services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C.  
17 § 2703(c). In doing so, Defendants have acted in excess of their statutory authority and in violation  
18 of statutory limitations.

19 238. AT&T acted as the agent of Defendants in performing, participating in, enabling,  
20 contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs'  
21 and class members' records or other information.

22 239. Defendants did not notify Plaintiffs or class members of the disclosure of these  
23 records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs  
24 or class members consent to such.

25 240. Plaintiffs and class members have been and are aggrieved by Defendants' above-  
26 described acts of soliciting and obtaining disclosure by AT&T of records or other information  
27 pertaining to Plaintiffs and class members.

28 241. On information and belief, the Count XIII Defendants are now engaging in and will  
continue to engage in the above-described soliciting and obtaining disclosure by AT&T of records  
or other information pertaining to Plaintiffs and class members, acting in excess of the Count XIII

1 Defendants' statutory authority and in violation of statutory limitations, including 18 U.S.C. §  
2 2703(c), and are thereby irreparably harming Plaintiffs and class members. Plaintiffs and class  
3 members have no adequate remedy at law for the Count XIII Defendants' continuing unlawful  
4 conduct, and the Count XIII Defendants will continue to violate Plaintiffs' and class members' legal  
5 rights unless enjoined and restrained by this Court.  
6

7 242. Pursuant to 18 U.S.C. § 2707, which provides a civil action for any person aggrieved  
8 by knowing or intentional violation of 18 U.S.C. § 2703, to *Larson v. United States*, 337 U.S. 682  
9 (1949), and to 5 U.S.C. § 702, Plaintiffs and class members seek equitable and declaratory relief  
10 against the Count XIII Defendants.

11 243. Plaintiffs seek that the Court declare that Defendants have violated their rights and  
12 the rights of the class; enjoin the Count XIII Defendants, their agents, successors, and assigns, and  
13 all those in active concert and participation with them from violating the Plaintiffs' and class  
14 members' statutory rights, including their rights under 18 U.S.C. § 2703; and award such other and  
15 further equitable relief as is proper.  
16

#### 17 COUNT XIV

#### 18 **Violation of 18 U.S.C. § 2703(c), actionable under 18 U.S.C. § 2707—Damages**

19 **(Named Plaintiffs vs. Defendants Alexander (in his personal capacity), Hayden (in his**  
20 **personal capacity), Cheney (in his personal capacity), Addington (in his personal capacity),**  
21 **Mukasey (in his personal capacity), Gonzales (in his personal capacity), Ashcroft (in his**  
22 **personal capacity), McConnell (in his personal capacity), and Negroponte (in his personal**  
23 **capacity), and one or more of the Doe Defendants)**

24 244. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
25 paragraphs of this complaint, as if set forth fully herein.

26 245. In relevant part, 18 U.S.C. § 2703(c) provides that:

27 (c) Records Concerning Electronic Communication Service or Remote  
28 Computing Service.—

(1) A governmental entity may require a provider of electronic  
communication service or remote computing service to disclose a record or

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

- (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
- (B) obtains a court order for such disclosure under subsection (d) of this section;
- (C) has the consent of the subscriber or customer to such disclosure;
- (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
- (E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

246. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- (C) has the consent of the subscriber or customer to such disclosure;
- (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
- (E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

- (A) name;
- (B) address;
- (C) local and long distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service utilized;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

253. Defendants intentionally and willfully solicited and obtained from AT&T, or aided, abetted, counseled, commanded, induced, procured, encouraged, promoted, instigated, advised, willfully caused, participated in, enabled, contributed to, facilitated, directed, controlled, assisted in, or conspired in the soliciting and obtaining from AT&T the disclosure to Defendants of records or other information pertaining to Plaintiffs' use of electronic communication services and/or remote computing services offered to the public by AT&T, in violation of 18 U.S.C. § 2703(c).

254. AT&T acted as the agent of Defendants in performing, participating in, enabling, contributing to, facilitating, or assisting in the commission of these acts of disclosure of Plaintiffs' records or other information.

255. Defendants did not notify Plaintiffs of the disclosure of these records or other information pertaining to them and their use of AT&T services, nor did Plaintiffs consent to such.







**JURY DEMAND**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: September 17, 2008



ELECTRONIC FRONTIER FOUNDATION  
CINDY COHN (1455997)  
LEE TIEN (148216)  
KURT OPSAHL (191303)  
KEVIN S. BANKSTON (217026)  
JAMES S. TYRE (083117)  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: 415/436-9333  
415/436-9993 (fax)

RICHARD R. WIEBE (121156)  
LAW OFFICE OF RICHARD R. WIEBE  
425 California Street, Suite 2025  
San Francisco, CA 94104  
Telephone: (415) 433-3200  
Facsimile: (415) 433-6382

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

Attorneys for Plaintiffs

# Exhibit B

# Exhibit B

1 CINDY COHN (SBN 145997)  
 cindy@eff.org  
 2 LEE TIEN (SBN 148216)  
 KURT OPSAHL (SBN 191303)  
 3 MATTHEW ZIMMERMAN (SBN 212423)  
 MARK RUMOLD (SBN 279060)  
 4 DAVID GREENE (SBN 160107)  
 JAMES S. TYRE (SBN 083117)  
 5 ELECTRONIC FRONTIER FOUNDATION  
 815 Eddy Street  
 6 San Francisco, CA 94109  
 Tel.: (415) 436-9333; Fax: (415) 436-9993  
 7 THOMAS E. MOORE III (SBN 115107)  
 8 tmoore@moorelawteam.com  
 ROYSE LAW FIRM, PC  
 9 1717 Embarcadero Road  
 Palo Alto, CA 94303  
 10 Tel.: 650-813-9700; Fax: 650-813-9777  
 11 Attorneys for Plaintiffs

RACHAEL E. MENY (SBN 178514)  
 rmeny@kvn.com  
 MICHAEL S. KWUN (SBN 198945)  
 BENJAMIN W. BERKOWITZ (SBN 244441)  
 KEKER & VAN NEST, LLP  
 633 Battery Street  
 San Francisco, California 94111  
 Tel.: (415) 391-5400; Fax: (415) 397-7188  
 RICHARD R. WIEBE (SBN 121156)  
 wiebe@pacbell.net  
 LAW OFFICE OF RICHARD R. WIEBE  
 One California Street, Suite 900  
 San Francisco, CA 94111  
 Tel.: (415) 433-3200; Fax: (415) 433-6382  
 ARAM ANTARAMIAN (SBN 239070)  
 aram@cff.org  
 LAW OFFICE OF ARAM ANTARAMIAN  
 1714 Blake Street  
 Berkeley, CA 94703  
 Telephone: (510) 289-1626

12  
 13 **UNITED STATES DISTRICT COURT**  
 14 **NORTHERN DISTRICT OF CALIFORNIA**  
 15 **SAN FRANCISCO DIVISION**

16 FIRST UNITARIAN CHURCH OF LOS )  
 ANGELES; ACORN ACTIVE MEDIA; BILL OF )  
 17 RIGHTS DEFENSE COMMITTEE; CALGUNS )  
 FOUNDATION, INC.; CALIFORNIA )  
 ASSOCIATION OF FEDERAL FIREARMS )  
 18 LICENSEES, INC.; CHARITY AND SECURITY )  
 NETWORK; COUNCIL ON AMERICAN )  
 19 ISLAMIC RELATIONS-CALIFORNIA; )  
 COUNCIL ON AMERICAN ISLAMIC )  
 20 RELATIONS-OHIO; COUNCIL ON )  
 AMERICAN ISLAMIC RELATIONS- )  
 21 FOUNDATION, INC.; FRANKLIN ARMORY; )  
 FREE PRESS; FREE SOFTWARE )  
 22 FOUNDATION; GREENPEACE, INC.; HUMAN )  
 RIGHTS WATCH; MEDIA ALLIANCE; )  
 23 NATIONAL LAWYERS GUILD; NATIONAL )  
 ORGANIZATION FOR THE REFORM OF )  
 24 MARIJUANA LAWS, CALIFORNIA CHAPTER;)  
 PATIENT PRIVACY RIGHTS; PEOPLE FOR )  
 25 THE AMERICAN WAY; PUBLIC )  
 KNOWLEDGE; SHALOM CENTER; )  
 26 STUDENTS FOR SENSIBLE DRUG POLICY; )  
 TECHFREEDOM; and UNITARIAN )  
 27 UNIVERSALIST SERVICE COMMITTEE, )  
 28 Plaintiffs. )

Case No: 3:13-cv-03287 JSW

**FIRST AMENDED COMPLAINT  
 FOR CONSTITUTIONAL AND  
 STATUTORY VIOLATIONS,  
 SEEKING DECLARATORY AND  
 INJUNCTIVE RELIEF**

Hon. Jeffrey S. White  
 Courtroom 11 - 19th Floor

**DEMAND FOR JURY TRIAL**











1           19. Plaintiff Bill of Rights Defense Committee (BORDC) is a non-profit, advocacy  
2 organization based in Northhampton, Massachusetts. BORDC supports an ideologically, politically,  
3 ethnically, geographically, and generationally diverse grassroots movement focused on educating  
4 Americans about the erosion of fundamental freedoms; increasing civic participation; and converting  
5 concern and outrage into political action. BORDC brings this action on behalf of itself and its  
6 adversely affected staff.

7           20. Plaintiff Calguns Foundation, Inc. (CGF) is a non-profit, membership organization  
8 based in San Carlos, California. CGF works to support the California firearms community by  
9 promoting education for all stakeholders about California and federal firearm laws, rights, and  
10 privileges, and defending and protecting the civil rights of California gun owners. In particular, CGF  
11 operates a hotline for those with legal questions about gun rights in California. Plaintiff CGF brings  
12 this action on behalf of itself and on behalf of its adversely affected members and staff.

13           21. Plaintiff California Association of Federal Firearms Licensees, Inc. (CAL-FFL) is a  
14 non-profit, industry association of, by, and for firearms manufacturers, dealers, collectors, training  
15 professionals, shooting ranges, and others, advancing the interests of its members and the general  
16 public through strategic litigation, legislative efforts, and education. CAL-FFL expends financial and  
17 other resources in both litigation and non-litigation projects to protect the interests of its members  
18 and the public at large. CAL-FFL brings this action on behalf of itself and its adversely affected  
19 members and staff.

20           22. Plaintiff Charity and Security Network's mission is to protect civil society's ability to  
21 carry out peacebuilding projects, humanitarian aid, and development work effectively and in a  
22 manner consistent with human rights principles and democratic values. To accomplish this, the  
23 Network focuses on: coordinating advocacy by bringing together stakeholders from across the  
24 nonprofit sector with policymakers to support needed changes in U.S. national security rules; and  
25 raising awareness, dispelling myths and promoting awareness of the positive contribution civil  
26 society makes to human security. CSN brings this action on behalf of itself and its adversely affected  
27 membership and staff.

28

1           23. Plaintiffs Council on American Islamic Relations – California (CAIR-CA), Council on  
2 American Islamic Relations-Ohio (CAIR-OHIO), and Council on American Islamic Relations-  
3 Foundation, Inc. (CAIR-F) are non-profit, advocacy organization with offices in California, Ohio,  
4 and Washington, D.C., respectively. CAIR-CA, CAIR-OHIO, and CAIR-F’s missions are to  
5 enhance the understanding of Islam, encourage dialogue, protect civil liberties, empower American  
6 Muslims, and build coalitions that promote justice and mutual understanding. CAIR-CA, CAIR-  
7 OHIO, and CAIR-F bring this action on behalf of themselves and their adversely affected staffs.

8           24. Plaintiff Franklin Armory, a wholly owned subsidiary of CBE, Inc., is a state and  
9 federally licensed manufacturer of firearms located in Morgan Hill, California. Franklin Armory  
10 specializes in engineering and building products for restrictive firearms markets, such as California.  
11 Franklin Armory is a member of CAL-FFL. Franklin Armory brings this suit on its own behalf.

12           25. Plaintiff Free Press is a non-profit, advocacy organization based in Washington, D.C.  
13 Free Press’s mission is to build a nationwide movement to change media and technology policies,  
14 promote the public interest, and strengthen democracy by advocating for universal and affordable  
15 Internet access, diverse media ownership, vibrant public media, and quality journalism. Free Press  
16 brings this action on behalf of itself and its adversely affected members and staff.

17           26. Plaintiff the Free Software Foundation (FSF) is a non-profit, membership organization  
18 based in Boston, Massachusetts. FSF helped pioneer a worldwide free software movement and  
19 provides an umbrella of legal and technical infrastructure for collaborative software development  
20 internationally. FSF brings this action on behalf of itself and its adversely affected members and  
21 staff.

22           27. Plaintiff Greenpeace, Inc. (Greenpeace) is a non-profit, membership organization  
23 headquartered in Washington, D.C. Through a domestic and international network of offices and  
24 staff, Greenpeace uses research, advocacy, public education, lobbying, and litigation to expose  
25 global environmental problems and to promote solutions that are essential to a green and peaceful  
26 future. Greenpeace brings this action on behalf of itself and its adversely affected members and staff.

27           28. Plaintiff Human Rights Watch (HRW) is a non-profit, advocacy organization, based in  
28

1 New York, New York. Through its domestic and international network of offices and staff, HRW  
2 challenges governments and those in power to end abusive practices and respect international human  
3 rights law by enlisting the public and the international community to support the cause of human  
4 rights for all. HRW brings this action on behalf of itself and its adversely affected staff.

5 29. Plaintiff Media Alliance is a non-profit, membership organization based in Oakland,  
6 California. Media Alliance serves as a resource and advocacy center for media workers, non-profit  
7 organizations, and social justice activists to make media accessible, accountable, decentralized,  
8 representative of society's diversity, and free from covert or overt government control and corporate  
9 dominance. Media Alliance brings this action on behalf of itself and its adversely affected members  
10 and staff.

11 30. Plaintiff National Lawyers Guild, Inc. is a non-profit corporation formed in 1937 as  
12 the nation's first racially integrated voluntary bar association. For over seven decades the Guild has  
13 represented thousands of Americans critical of government policies, from antiwar, environmental  
14 and animal rights activists, to Occupy Wall Street protesters, to individuals accused of computer-  
15 related offenses. From 1940-1975 the FBI conducted a campaign of surveillance, investigation and  
16 disruption against the Guild and its members, trying unsuccessfully to label it a subversive  
17 organization. The NLG brings this action on behalf of itself and its adversely affected membership  
18 and staff.

19 31. Plaintiff National Organization for the Reform of Marijuana Laws, California Chapter  
20 (NORML, California Chapter) is a non-profit, membership organization located in Berkeley,  
21 California. NORML, California Chapter is dedicated to reforming California's marijuana laws and  
22 its mission is to establish the right of adults to use cannabis legally. NORML, California Chapter  
23 brings this action on behalf of itself and its adversely affected members and staff.

24 32. Plaintiff Patient Privacy Rights (PPR) is a bipartisan, non-profit organization with  
25 12,000 members in all 50 states. It works to give patients control over their own sensitive health  
26 information in electronic systems, with the goal of empowering privacy and choices that protect jobs  
27 and opportunities and ensure trust in the patient-physician relationship. The lack of privacy of health  
28

1 information causes millions of individuals every year to refuse or delay needed medical treatment or  
2 hide information, putting their health at risk. PPR brings this action on behalf of itself and its  
3 adversely affected members and volunteers.

4 33. Plaintiff People for the American Way (PFAW) is a non-profit, membership  
5 organization based in Washington, D.C. With over 595,000 members, PFAW's primary function is  
6 the education of its members, supporters, and the general public as to important issues that impact  
7 fundamental civil and constitutional rights and freedoms, including issues concerning civil liberties,  
8 government secrecy, improper government censorship, and First Amendment freedoms. PFAW  
9 brings this action on behalf of itself and its adversely affected members and staff.

10 34. Plaintiff Public Knowledge is a non-profit, advocacy organization based in  
11 Washington, D.C. Public Knowledge is dedicated to preserving the openness of the Internet and the  
12 public's access to knowledge, promoting creativity through the balanced application of copyright  
13 laws, and upholding and protecting the rights of consumers to use innovative technology lawfully.  
14 Public Knowledge brings this action on behalf of itself and its adversely affected staff.

15 35. Plaintiff the Shalom Center seeks to be a prophetic voice in Jewish, multireligious, and  
16 American life. It connects the experience and wisdom of the generations forged in the social,  
17 political, and spiritual upheavals of the last half-century with the emerging generation of activists,  
18 addressing with special concern the planetary climate crisis and the power configurations behind that  
19 crisis. The Shalom Center brings this action on behalf of itself and its adversely affected membership  
20 and staff.

21 36. Plaintiff Students for Sensible Drug Policy (SSDP) is a non-profit, membership  
22 organization based in Washington, D.C. With over 3,000 members, SSDP is an international,  
23 grassroots network of students who are concerned about the impact drug abuse has on our  
24 communities, but who also know that the War on Drugs is failing our generation and our society.  
25 SSDP creates change by bringing young people together and creating safe spaces for students of all  
26 political and ideological stripes to have honest conversations about drugs and drug policy. SSDP  
27 brings this action on behalf of itself and its adversely affected membership and staff.

28



1           37. Plaintiff TechFreedom is a non-profit, think tank based in Washington, D.C.  
2 TechFreedom's mission is promoting technology that improves the human condition and expands  
3 individual capacity to choose by educating the public, policymakers, and thought leaders about the  
4 kinds of public policies that enable technology to flourish. TechFreedom seeks to advance public  
5 policy that makes experimentation, entrepreneurship, and investment possible, and thus unleashes  
6 the ultimate resource: human ingenuity. TechFreedom brings this action on behalf of itself and its  
7 adversely affected staff.

8           38. Plaintiff Unitarian Universalist Service Committee (UUSC) is a non-profit,  
9 membership organization based in Cambridge, Massachusetts. UUSC advances human rights and  
10 social justice around the world, partnering with those who confront unjust power structures and  
11 mobilizing to challenge oppressive policies. Through a combination of advocacy, education, and  
12 partnerships with grassroots organizations, UUSC promotes economic rights, advances  
13 environmental justice, defends civil liberties, and preserves the rights of people in times of  
14 humanitarian crisis. UUSC brings this action on behalf of itself and its adversely affected members  
15 and staff.

16           39. All Plaintiffs make and receive telephone calls originating within the United States in  
17 furtherance of their mission and operations. In particular, Plaintiffs make and receive telephone calls  
18 to and from their members, staffs, and constituents, among other groups and individuals seeking to  
19 associate with them, in furtherance of their mission and operations, including advancing their  
20 political beliefs, exchanging ideas, and formulating strategy and messages in support of their causes.

21           40. Each of the Plaintiffs above is a membership organization and brings this action on  
22 behalf of its members has members whose communications information has been collected as part of  
23 the Associational Tracking Program.

24           41. Defendant NSA is an agency under the direction and control of the Department of  
25 Defense that seizes, collects, processes, and disseminates signals intelligence. It is responsible for  
26 carrying out at least some of the Associational Tracking Program challenged herein.

27           42. Defendant General Keith B. Alexander is the current Director of the NSA, in office  
28

1 since April of 2005. As NSA Director, General Alexander has authority for supervising and  
2 implementing all operations and functions of the NSA, including the Associational Tracking  
3 Program. General Alexander personally authorizes and supervises the Associational Tracking  
4 Program.

5 43. Defendant United States is the United States of America, its departments, agencies,  
6 and entities.

7 44. Defendant Department of Justice is a Cabinet-level executive department in the United  
8 States government charged with law enforcement, defending the interests of the United States  
9 according to the law, and ensuring fair and impartial administration of justice for all Americans.

10 45. Defendant Eric H. Holder is the current Attorney General of the United States, in  
11 office since February of 2009. Attorney General Holder personally approves, authorizes, supervises,  
12 and participates in the Associational Tracking Program on behalf of the Department of Justice.

13 46. Defendant John B. Carlin is the current Acting Assistant Attorney General for  
14 National Security. In that position, defendant Carlin participates in the Department of Justice's  
15 implementation of the Associational Tracking Program.

16 47. Defendant Federal Bureau of Investigation (FBI) is a component of the Department of  
17 Justice that conducts federal criminal investigation and collects domestic intelligence. FBI is  
18 responsible for carrying out at least some of the Associational Tracking Program activities  
19 challenged herein.

20 48. Defendant James B. Comey is the current Director of the FBI, in office since  
21 September of 2013. As FBI Director, defendant Comey has ultimate authority for supervising and  
22 implementing all operations and functions of the FBI, including its participation in the Associational  
23 Tracking Program. Defendant Comey personally authorizes and supervises the FBI's participation in  
24 the Associational Tracking Program.

25 49. Defendant Robert S. Mueller is the previous Director of the FBI, from September,  
26 2001-September, 2013. As FBI Director, defendant Mueller had ultimate authority for supervising  
27 and implementing all operations and functions of the FBI, including its participation in the  
28

1 Associational Tracking Program. Defendant Mueller personally authorized and supervised the FBI's  
2 participation in the Associational Tracking Program.

3 50. Defendant Lieutenant General (Ret.) James R. Clapper is the Director of National  
4 Intelligence (DNI), in office since August of 2010. Defendant Clapper participates in the activities of  
5 the U.S. intelligence community, including the Associational Tracking Program.

6 51. Defendants DOES 1-100 are persons or entities who have authorized or participated in  
7 the Associational Tracking Program. Plaintiffs will allege their true names and capacities when  
8 ascertained. Upon information and belief each is responsible in some manner for the occurrences  
9 herein alleged and the injuries to Plaintiffs herein alleged were proximately caused by the acts or  
10 omissions of DOES 1-100 as well as the named Defendants.

11 **FACTUAL ALLEGATIONS RELATED TO ALL COUNTS**

12 **STATUTORY BACKGROUND**

13 52. 50 U.S.C § 1861, the codification of section 215 of the USA PATRIOT Act, as  
14 amended, is entitled "Access to certain business records for foreign intelligence and surveillance  
15 purposes." Section 1861 provides narrow and limited authority for the Foreign Intelligence  
16 Surveillance Court (FISC) to issue orders for the production of "any tangible things (including  
17 books, records, papers, documents, and other items) for an investigation to obtain foreign  
18 intelligence information not concerning a United States person or to protect against international  
19 terrorism or clandestine intelligence activities." The limitations on section 1861 orders include the  
20 following:

- 21 • an order may be issued only upon "a statement of facts showing that there are  
22 reasonable grounds to believe that the tangible things sought are relevant to an  
23 authorized investigation;"
- 24 • the tangible things sought to be produced by an order must be described "with  
25 sufficient particularity to permit them to be fairly identified;" and
- 26 • an order "may only require the production of a tangible thing if such thing can be  
27 obtained with a *subpoena duces tecum* issued by a court of the United States in aid of  
28

1 a grand jury investigation or with any other order issued by a court of the United  
2 States directing the production of records or tangible things.”

3 **THE ASSOCIATIONAL TRACKING PROGRAM**

4 53. The Associational Tracking Program is electronic surveillance that collects and  
5 acquires telephone communications information for all telephone calls transiting the networks of all  
6 major American telecommunication companies, including Verizon, AT&T, and Sprint. Every day,  
7 the Associational Tracking Program collects information about millions of telephone calls made by  
8 millions of Americans. This includes information about all calls made wholly within the United  
9 States, including local telephone calls, as well as communications between the United States and  
10 abroad.

11 54. Defendants’ Associational Tracking Program collects and acquires call detail records  
12 and comprehensive communications routing information about telephone calls. The collected  
13 information includes, but is not limited to, session identifying information (*e.g.*, originating and  
14 terminating telephone number, International Mobile Subscriber Identity (IMSI) number,  
15 International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone  
16 calling card numbers, and time and duration of call. Defendants acquire this information through the  
17 use of a surveillance device.

18 55. Beginning in 2001, participating phone companies voluntarily provided telephone  
19 communications information for the Associational Tracking program to Defendants. Since 2006, the  
20 FISC, at the request of Defendants, has issued orders under 50 U.S.C. § 1861 purporting to compel  
21 the production of communications information, including communications information not yet in  
22 existence, on an ongoing basis, as part of the Associational Tracking Program.

23 56. As an example, attached hereto as Exhibit A, and incorporated herein by this  
24 reference, is an Order issued under 50 U.S.C. § 1861 requiring the production of communications  
25 information for use in the Associational Tracking Program.

26 57. DNI Clapper has admitted the Order is authentic, as indicated in Exhibit B, attached  
27 hereto and incorporated by this reference.

1           58.     The Order is addressed to Verizon Business Network Services Inc., on behalf of MCI  
2 Communications Services Inc., d/b/a Verizon Business Services (individually and collectively  
3 “Verizon”). Verizon is one of the largest providers of telecommunications services in the United  
4 States with over 98 million subscribers. Through its subsidiaries and other affiliated entities that it  
5 owns, controls, or provides services to, Verizon provides telecommunications services to the public  
6 and to other entities. These subsidiaries and affiliated entities include Verizon Business Global,  
7 LLC; MCI Communications Corporation; Verizon Business Network Services, Inc.; MCI  
8 Communications Services, Inc.; and Verizon Wireless (Cellco Partnership).

9                           **BULK SEIZURE COLLECTION, ACQUISITION, AND STORAGE**

10           59.     The Associational Tracking Program seizes, collects and acquires telephone  
11 communications information for all telephone calls transiting the networks of all major American  
12 telecommunication companies, including Verizon, AT&T, and Sprint.

13           60.     The telephone communications information Defendants seize, collect and acquire in  
14 bulk as part of the Associational Tracking Program is retained and stored by Defendants in one or  
15 more databases. These databases contain call information for all, or the vast majority, of calls wholly  
16 within the United States, including local telephone calls, and calls between the United States and  
17 abroad, for a period of at least five years. Defendants have indiscriminately obtained and stored the  
18 telephone communications information of millions of ordinary Americans, including Plaintiffs, their  
19 members, and staffs, as part of the Associational Tracking Program.

20           61.     Defendants’ bulk seizure, collection and acquisition of telephone communications  
21 information includes, but is not limited to, records indicating who each customer communicates  
22 with, at what time, and for how long. The aggregation of this information discloses the expressive,  
23 political, social, personal, private, and intimate associational connections among individuals and  
24 groups, which ordinarily would not be disclosed to the public or the government.

25           62.     Through the Associational Tracking Program, Defendants have seized, collected,  
26 acquired, and retained, and continue to seize, collect, acquire, and retain, bulk communications  
27 information of telephone calls made and received by Plaintiffs, their members, and their staffs. This  
28

1 information is otherwise private.

2 63. Because of the Associational Tracking Program, Plaintiffs have lost the ability to  
3 assure confidentiality in the fact of their communications to their members and constituent.  
4 Plaintiffs' associations and political advocacy efforts, as well as those of their members and staffs,  
5 are chilled by the fact that the Associational Tracking Program creates a permanent record of all of  
6 Plaintiffs' telephone communications with their members and constituents, among others.

7 64. Plaintiffs' associations and political advocacy efforts, as well as those of their  
8 members and staffs, are chilled by Defendants' search and analysis of information obtained through  
9 the Associational Tracking Program and Defendants' use and disclose of this information and the  
10 results of their searches and analyses.

11 65. Plaintiffs' telephone communications information obtained, retained, and searched  
12 pursuant to the Associational Tracking Program was at the time of acquisition, and at all times  
13 thereafter, neither relevant to an existing authorized criminal investigation nor to an existing  
14 authorized investigation to protect against international terrorism or clandestine intelligence  
15 activities.

16 66. Defendants' bulk seizure, collection, acquisition, and retention of the telephone  
17 communications information of Plaintiffs, their members, and their staffs is done without lawful  
18 authorization, probable cause, and/or individualized suspicion. It is done in violation of statutory and  
19 constitutional limitations and in excess of statutory and constitutional authority. Any judicial,  
20 administrative, or executive authorization (including any order issued pursuant to the business  
21 records provision of 50 U.S.C. § 1861) of the Associational Tracking Program or of the acquisition  
22 and retention of the communications information of Plaintiffs, their members, and their staffs is  
23 unlawful and invalid.

24 67. Defendants' bulk seizure, collection, acquisition, and retention of the telephone  
25 communications information of Plaintiffs, their members, and their staffs is done (a) without  
26 probable cause or reasonable suspicion to believe that Plaintiffs, their members, and their staffs have  
27 committed or are about to commit any crime or engage in any international terrorist activity; (b)

28

1 without probable cause or reasonable suspicion to believe that Plaintiffs, their members, or their  
2 staffs are foreign powers or agents of foreign powers; and (c) without probable cause or reasonable  
3 suspicion to believe that the communications of Plaintiffs, their members, and their staffs contain or  
4 pertain to foreign intelligence information, or relate to an investigation to obtain foreign intelligence  
5 information.

6 68. Defendants, and each of them, have authorized, approved, supervised, performed,  
7 caused, participated in, aided, abetted, counseled, commanded, induced, procured, enabled,  
8 contributed to, facilitated, directed, controlled, assisted in, or conspired in the Associational Tracking  
9 Program and in the seizure, collection, acquisition, and retention of the telephone communications  
10 information of Plaintiffs, their members, and their staffs. Defendants have committed these acts  
11 willfully, knowingly, and intentionally. Defendants continue to commit these acts and will continue  
12 to do so absent an order of this Court enjoining and restraining them from doing so.

#### 13 SEARCH

14 69. Through the Associational Tracking Program, Defendants have searched and continue  
15 to search communications information of telephone calls made and received by Plaintiffs, their  
16 members, and their staffs. Defendants use the communications information acquired for the  
17 Associational Tracking Program for a process known as “contact chaining” — the construction of an  
18 associational network graph that models the communication patterns of people, organizations, and  
19 their associates.

20 70. As part of the Associational Tracking Program, contact chains are created both in an  
21 automated fashion and based on particular queries. Contact chain analyses are typically performed  
22 for two degrees of separation (or two “hops”) away from an intended target. That is, an associational  
23 network graph would be constructed not just for the target of a particular query, but for any number  
24 in direct contact with that target, and any number in contact with a direct contact of the target.  
25 Defendants sometimes conduct associational analyses up to three degrees of separation (“three  
26 hops”) away.

27 71. The searches include Plaintiffs’ communications information even if plaintiffs are not  
28

1 targets of the government and even if they are not one, two or more “hops” away from a target. All  
2 telephone communications information is searched as part of the Associational Tracking Program.

3 72. Plaintiffs’ telephone communications information searched pursuant to the  
4 Associational Tracking Program was, at the time of search and at all times thereafter, was neither  
5 relevant to an existing authorized criminal investigation nor to an existing authorized investigation to  
6 protect against international terrorism or clandestine intelligence activities.

7 73. Defendants’ searching of the telephone communications information of Plaintiffs is  
8 done without lawful authorization, probable cause, and/or individualized suspicion. It is done in  
9 violation of statutory and constitutional limitations and in excess of statutory and constitutional  
10 authority. Any judicial, administrative, or executive authorization (including any business records  
11 order issued pursuant 50 U.S.C. § 1861) of the Associational Tracking Program or of the searching  
12 of the communications information of Plaintiffs is unlawful and invalid.

13 74. Defendants’ searching of the telephone communications information of Plaintiffs is  
14 done (a) without probable cause or reasonable suspicion to believe that Plaintiffs, their members, or  
15 their staffs, have committed or are about to commit any crime or engage in any international terrorist  
16 activity; (b) without probable cause or reasonable suspicion to believe that Plaintiffs, their members,  
17 or their staffs are foreign powers or agents of foreign powers; and (c) without probable cause or  
18 reasonable suspicion to believe that Plaintiffs’, their members’, or their staffs’ communications  
19 contain or pertain to foreign intelligence information or relate to an investigation to obtain foreign  
20 intelligence information.

21 75. Defendants, and each of them, have authorized, approved, supervised, performed,  
22 caused, participated in, aided, abetted, counseled, commanded, induced, procured, enabled,  
23 contributed to, facilitated, directed, controlled, assisted in, or conspired in the Associational Tracking  
24 Program and in the search or use of the telephone communications information of Plaintiffs, their  
25 members, and their staff. Defendants have committed these acts willfully, knowingly, and  
26 intentionally. Defendants continue to commit these acts and will continue to do so absent an order of  
27 this Court enjoining and restraining them from doing so.

28



**INJURY COMMON TO ALL PLAINTIFFS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

76. Each and every Plaintiff is informed and believes that its associational activities have been harmed since the existence of the Associational Tracking Program became publicly known. Each Plaintiff has experienced a decrease in communications from members and constituents who had desired the fact of their communication to Plaintiff to remain secret, especially from the government and its various agencies, or has heard employees, members or associates express concerns about the confidentiality of the fact of their communications with Plaintiffs. Those Plaintiffs who operate hotlines have observed a decrease in calls to the hotlines and/or an increase in callers expressing concern about the confidentiality of the fact of their communications. Since the disclosure of the Associational Tracking Program, Plaintiffs have lost the ability to assure their members and constituents, as well as all others who seek to communicate with them, that the fact of their communications to Plaintiffs will be kept confidential, especially from the federal government, including its various agencies. This injury stems not from the disclosure of the Associational Tracking Program, but from the existence and operation of the program itself. Before the public disclosure of the program, Plaintiffs' assurances of confidentiality were illusory.

77. For instance, these specific Plaintiffs experienced the following:

(a) Plaintiff First Unitarian has a proud history of working for justice and protecting people in jeopardy for expressing their political views. In the 1950s, it resisted the McCarthy hysteria and supported blacklisted Hollywood writers and actors, and fought California's 'loyalty oaths' all the way to the Supreme Court. And in the 1980s, it gave sanctuary to refugees from civil wars in Central America. The principles of its faith often require the church to take bold stands on controversial issues. Church members and neighbors who come to the church for help should not fear that their participation in the church might have consequences for themselves or their families. This spying makes people afraid to belong to the church community.

(b) Plaintiff Calguns Foundation runs a hotline for that allows the general public to call to ask questions about California's byzantine firearms laws. It has members who would be very worried about having their calls taped and stored by NSA/FBI when they're enquiring about

1 whether firearms and parts they possess are felonious in California. It has a phone number  
2 specifically so people or their loved ones can call from jail because Californians are often arrested  
3 for actually innocent possession or use of firearms.

4 (c) Plaintiff NLG notes that much of its work involves cases (some high profile)  
5 involving individuals who have been charged with aiding terrorism or who have been monitored by  
6 the FBI and Joint Terrorism Task Forces for their political activism. Knowledge that its email and  
7 telephonic communications may likely be monitored has resulted in restricting what its employees  
8 and members say over the telephone and in email about legal advocacy and work related to NLG  
9 litigation or legal defense committees. In several instances, it has had to convene in-person meetings  
10 to discuss sensitive matters. One example is its "Green Scare" hotline for individuals contacted by  
11 the FBI, either as targets or in relation to environmental or animal rights cases. NLG immediately  
12 advises Hotline callers that the line may not be secure, asks limited information before referring  
13 callers to specific NLG attorneys in their geographic area, and does not keep notes or records of the  
14 calls. One foundation funder asks for records of Hotline calls, but in response the NLG can only send  
15 general examples of the types of calls it receives.

16 (d) Plaintiff Human Rights Watch conducts research and advocacy such that its  
17 effectiveness and credibility depend heavily on being able to interview those with direct knowledge  
18 of human rights abuses, be they victims, witnesses, perpetrators, or knowledgeable bystanders such  
19 as government officials, humanitarian agencies, lawyers and other civil society partners. Because  
20 this type of research and reporting can endanger people and organizations, our stakeholders—  
21 including even our researchers and/or consultants--often require us to keep their identities or other  
22 identifying information confidential. HRW has staff in these offices who talk to the above-  
23 mentioned types of stakeholders by telephone to conduct research. HRW is concerned that many of  
24 these stakeholders will have heightened concerns about contacting us through our offices now that  
25 we are aware the NSA is logging metadata of these calls. This impairs HRW's research ability  
26 and/or causes HRW to rely more on face-to-face encounters or other costly means of holding secure  
27 conversations.

28

1 (e) Plaintiff Shalom Center’s Executive Director, Rabbi Arthur Waskow, was  
2 subjected to COINTELPRO activity (warrantless searches, theft, forgery) by the FBI between 1968  
3 and 1974. He took part in a suit against the FBI and the Washington DC police (*Hobson v. Wilson*)  
4 for deprivation of the “right of the people peaceably to assemble.” Rabbi Waskow won in DC  
5 Federal District Court and the part of the suit that focused on the FBI was upheld in the DC Circuit  
6 Court of Appeals. The result of this experience is that he has been very troubled and frightened by  
7 the revelations of warrantless mass searches of telephone and Internet communications by the NSA.  
8 For several weeks, as the revelations continued, Rabbi Waskow realized the likelihood that the  
9 organization he leads, the Shalom Center, and he were under illegitimate surveillance and —  
10 because of its involvement in legal and nonviolent opposition to US government policy in several  
11 fields — possibly worse. This realization made him rethink whether he wanted to continue in sharp  
12 prophetic criticism and action in regard to disastrous public policies. Rabbi Waskow had trouble  
13 sleeping, delayed some essays and blogs he had been considering, and worried whether his actions  
14 might make trouble for nonpolitical relatives. Rabbi Waskow certainly felt a chill fall across his  
15 work of peaceable assembly, association, petition, and the free exercise of his religious convictions.

16 **COUNT I**

17 **Violation of First Amendment—Declaratory, Injunctive, and Other Equitable Relief**  
18 **(Against All Defendants)**

19 78. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding  
20 paragraphs of this complaint, as if set forth fully herein.

21 79. Plaintiffs, their members, and their staffs use telephone calls to communicate and to  
22 associate within their organization, with their members and with others, including to communicate  
23 anonymously and to associate privately.

24 80. By their acts alleged herein, Defendants have violated and are violating the First  
25 Amendment free speech and free association rights of Plaintiffs, their members, and their staffs,  
26 including the right to communicate anonymously, the right to associate privately, and the right to  
27 engage in political advocacy free from government interference.

28 81. By their acts alleged herein, Defendants have chilled and/or threaten to chill

1 the legal associations and speech of Plaintiffs, their members, and their staffs by, among other  
2 things, compelling the disclosure of their political and other associations, and eliminating Plaintiffs'  
3 ability to assure members and constituents that the fact of their communications with them will be  
4 kept confidential.

5 82. Defendants are irreparably harming Plaintiffs, their members, and their staffs by  
6 violating their First Amendment rights. Plaintiffs have no adequate remedy at law for Defendants'  
7 continuing unlawful conduct, and Defendants will continue to violate Plaintiffs' legal rights unless  
8 enjoined and restrained by this Court.

9 83. Plaintiffs seek that this Court declare that Defendants have violated the First  
10 Amendment rights of Plaintiffs, their members, and their staffs; enjoin Defendants, their agents,  
11 successors, and assigns, and all those in active concert and participation with them from violating the  
12 First Amendment to the United States Constitution; and award such other and further equitable relief  
13 as is proper.

## 14 **COUNT II**

### 15 **Violation of Fourth Amendment—Declaratory, Injunctive, and Equitable Relief** 16 **(Against All Defendants)**

17 84. Plaintiffs repeat and incorporate herein by reference the allegations in paragraphs 1  
18 through 66 of this complaint, as if set forth fully herein.

19 85. Plaintiffs have a reasonable expectation of privacy in their telephone communications,  
20 including in their telephone communications information.

21 86. By the acts alleged herein, Defendants have violated Plaintiffs' reasonable  
22 expectations of privacy and denied Plaintiffs their right to be free from unreasonable searches and  
23 seizures as guaranteed by the Fourth Amendment to the Constitution of the United States, including,  
24 but not limited to, obtaining *per se* unreasonable general warrants. Defendants have further violated  
25 Plaintiffs' rights by failing to apply to a court for, and for a court to issue, a warrant prior to any  
26 search and seizure as guaranteed by the Fourth Amendment.

27 87. Defendants are now engaging in and will continue to engage in the above-described  
28 violations of Plaintiffs' constitutional rights, and are thereby irreparably harming Plaintiffs.

1 Plaintiffs have no adequate remedy at law for Defendants' continuing unlawful conduct, and  
2 Defendants will continue to violate Plaintiffs' legal rights unless enjoined and restrained by this  
3 Court.

4 88. Plaintiffs seek that this Court declare that Defendants have violated their Fourth  
5 Amendment rights; enjoin Defendants, their agents, successors, and assigns, and all those in active  
6 concert and participation with them from violating the Plaintiffs' rights under the Fourth  
7 Amendment to the United States Constitution; and award such other and further equitable relief as is  
8 proper.

9 **COUNT III**

10 **Violation of Fifth Amendment—Declaratory, Injunctive, and Equitable Relief**  
11 **(Against All Defendants)**

12 89. Plaintiffs repeat and incorporate herein by reference the allegations in paragraphs 1  
13 through 66 of this complaint, as if set forth fully herein.

14 90. Plaintiffs, their members, and their staffs have an informational privacy interest in  
15 their telephone communications information, which reveals sensitive information about their  
16 personal, political, and religious activities and which Plaintiffs do not ordinarily disclose to the  
17 public or the government. This privacy interest is protected by state and federal laws relating to  
18 privacy of communications records and the substantive and procedural right to due process  
19 guaranteed by the Fifth Amendment.

20 91. Defendants through their Associational Tracking Program secretly seize, collect,  
21 acquire, retain, search, and use the bulk telephone communications information of Plaintiffs, their  
22 members, and their staff without providing notice to them, or process by which they could seek  
23 redress. Defendants provide no process adequate to protect their interests.

24 92. Defendants seize, collect, acquire, retain, search, and use the bulk telephone  
25 communications information of Plaintiffs, their members, and their staff without making any  
26 showing of any individualized suspicion, probable cause, or other governmental interest sufficient or  
27 narrowly tailored to justify the invasion of Plaintiffs' due process right to informational privacy.

28 93. Defendants seize, and acquire the bulk telephone communications information of

1 Plaintiffs, their members, and their staff under, *inter alia*, section 215 of the USA-PATRIOT Act (50  
2 U.S.C. § 1861).

3 94. On information and belief, Defendants' information seizure, collection and acquisition  
4 activities rely on a secret legal interpretation of 50 U.S.C. § 1861 under which bulk telephone  
5 communications information of persons generally is as a matter of law deemed a "tangible thing"  
6 "relevant" to "an investigation to obtain foreign intelligence information not concerning a United  
7 States person or to protect against international terrorism or clandestine intelligence activities," even  
8 without any particular reason to believe that telephone communications information is a "tangible  
9 thing" or that the telephone communications information of any particular person, including  
10 Plaintiffs, their members, and their staff, is relevant to an investigation to obtain foreign intelligence  
11 information not concerning a U.S. person or to protect against international terrorism or clandestine  
12 intelligence activities.

13 95. This legal interpretation of 50 U.S.C. § 1861 is not available to the general public,  
14 including Plaintiffs, their members, and their staff, leaving them and all other persons uncertain  
15 about where a reasonable expectation of privacy from government intrusion begins and ends and  
16 specifically what conduct may subject them to electronic surveillance.

17 96. This secret legal interpretation of 50 U.S.C. § 1861, together with provisions of the  
18 FISA statutory scheme that insulate legal interpretations from public disclosure and adversarial  
19 process, fails to establish minimal guidelines to govern law enforcement and/or intelligence seizure  
20 and collection.

21 97. The secret legal interpretation of 50 U.S.C. § 1861 used in the Associational Tracking  
22 Program and related surveillance programs causes section 1861 to be unconstitutionally vague in  
23 violation of the Fifth Amendment and the rule of law. The statute on its face gives no notice that it  
24 could be construed to authorize the bulk seizure and collection of telephone communications  
25 information for use in future investigations that do not yet exist.

26 98. By these and the other acts alleged herein, Defendants have violated and are  
27 continuing to violate the right to due process under the Fifth Amendment of Plaintiffs, their  
28

1 members, and their staff.

2 99. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs.

3 100. On information and belief, Defendants are now engaging in and will continue to  
4 engage in the above-described violations of Plaintiffs' constitutional rights, and are thereby  
5 irreparably harming Plaintiffs. Plaintiffs have no adequate remedy at law for Defendants' continuing  
6 unlawful conduct, and Defendants will continue to violate Plaintiffs' legal rights unless enjoined and  
7 restrained by this Court.

8 101. Plaintiffs seek that this Court declare that Defendants have violated their due process  
9 rights under the Fifth Amendment to the United States Constitution; enjoin Defendants, their agents,  
10 successors, and assigns, and all those in active concert and participation with them from violating the  
11 Plaintiffs' due process rights; and award such other and further equitable relief as is proper.

12 **COUNT IV**

13 **Violation of 50 U.S.C. § 1861—Declaratory, Injunctive and Other Equitable Relief**  
14 **(Against All Defendants)**

15 102. Plaintiffs repeat and incorporate herein by reference the allegations in paragraph 1  
16 through 66 of this complaint, as if set forth fully herein.

17 103. The business records order provision set forth in 50 U.S.C. § 1861 limits Defendants'  
18 ability to seek telephone communications information. It does not permit the suspicionless bulk  
19 seizure and collection of telephone communications information unconnected to any ongoing  
20 investigation. It does not permit an order requiring the production of intangible things, including  
21 telephone communications information not yet in existence.

22 104. Defendants' Associational Tracking Program and the seizure, collection, acquisition,  
23 retention, searching, and use of the telephone communications records of Plaintiffs, their members,  
24 and their staff exceed the conduct that may be lawfully authorized by an order issued under 50 U.S.C  
25 § 1861.

26 105. By the acts alleged herein, Defendants are acting in excess of their statutory authority  
27 and in violation of the express statutory limitations and procedures Congress has imposed on them in  
28 50 U.S.C. § 1861.

1 106. Sovereign immunity for this claim is waived by 5 U.S.C. § 702.

2 107. Defendants are now engaging in and will continue to engage in the above-described  
3 acts in excess of Defendants' statutory authority and in violation of statutory limitations and  
4 procedures of 50 U.S.C. § 1861 and are thereby irreparably harming Plaintiffs. Plaintiffs have no  
5 adequate remedy at law for Defendants' continuing unlawful conduct, and Defendants will continue  
6 to violate Plaintiffs' legal rights unless enjoined and restrained by this Court.

7 108. Plaintiffs seek that this Court declare that Defendants have acted in excess of  
8 Defendants' statutory authority and in violation of statutory limitations and procedures of 50 U.S.C.  
9 § 1861; declare that Defendants have thereby irreparably harmed and will continue to irreparably  
10 harm Plaintiffs; enjoin Defendants, their agents, successors, and assigns, and all those in active  
11 concert and participation with them from acting in excess of Defendants' statutory authority and in  
12 violation of statutory limitations and procedures of 50 U.S.C. § 1861; and award such other and  
13 further equitable relief as is proper.

14 **COUNT V**

15 **Motion For Return Of Unlawfully Searched And Seized Property Pursuant To**  
16 **Federal Rule of Criminal Procedure 41(g)**

17 109. Plaintiffs repeat and incorporate herein by reference the allegations in paragraphs 1  
18 through 97 of this complaint, as if set forth fully herein.

19 110. This Court has civil equitable jurisdiction under Federal Rule of Criminal  
20 Procedure 41(g) to order the return of illegally searched and seized property.

21 111. Defendants, by their Associational Tracking Program and their bulk seizure,  
22 collection, acquisition, retention, searching, and use of the telephone communications information of  
23 Plaintiffs, have unlawfully searched and seized Plaintiffs' telephone communications information.  
24 Plaintiffs are aggrieved by Defendants unlawful seizure and search of their telephone  
25 communications information.

26 112. Plaintiffs seek an order directing the return of their telephone communications  
27 information in the possession, custody, or control of Defendants, their agents, successors, and  
28 assigns, and all those in active concert and participation with them.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs respectfully request that the Court:

1. Declare that the Program as alleged herein violates without limitation Plaintiffs’ rights under the First, Fourth, and Fifth Amendments to the Constitution; and their statutory rights;
2. Award to Plaintiffs equitable relief, including without limitation, a preliminary and permanent injunction pursuant to the First, Fourth, and Fifth Amendments to the United States Constitution prohibiting Defendants’ continued use of the Program, and a preliminary and permanent injunction pursuant to the First, Fourth, and Fifth Amendments requiring Defendants to provide to Plaintiffs an inventory of their communications, records, or other information that was seized in violation of the First, Fourth, and Fifth Amendments, and further requiring the destruction of all copies of those communications, records, or other information within the possession, custody, or control of Defendants.
3. Award to Plaintiffs reasonable attorneys’ fees and other costs of suit to the extent permitted by law.
4. Order the return and destruction of their telephone communications information in the possession, custody, or control of Defendants, their agents, successors, and assigns, and all those in active concert and participation with them.
5. Grant such other and further relief as the Court deems just and proper.

DATED: September 10, 2013

Respectfully submitted,

/s/ Cindy Cohn  
 CINDY COHN  
 LEE TIEN  
 KURT OPSAHL  
 MATTHEW ZIMMERMAN  
 MARK RUMOLD  
 DAVID GREENE  
 JAMES S. TYRE  
 ELECTRONIC FRONTIER FOUNDATION

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

RICHARD R. WIEBE  
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III  
THE MOORE LAW GROUP

RACHAEL E. MENY  
MICHAEL S. KWUN  
BENJAMIN W. BERKOWITZ  
KEKER & VAN NEST, LLP

ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**JURY DEMAND**

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: September 10, 2013

Respectfully submitted,

/s/ Cindy Cohn  
CINDY COHN  
LEE TIEN  
KURT OPSAHL  
MATTHEW ZIMMERMAN  
MARK RUMOLD  
DAVID GREENE  
JAMES S. TYRE  
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE  
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III  
THE MOORE LAW GROUP

RACHAEL E. MENY  
MICHAEL S. KWUN  
BENJAMIN W. BERKOWITZ  
KEKER & VAN NEST, LLP

ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs

# Exhibit C

# Exhibit C

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

CAROLYN JEWEL *et al.*,

*Plaintiffs,*

v.

NATIONAL SECURITY AGENCY *et al.*,

*Defendants*

Case No. C:08-cv-4373-VRW

Chief Judge Vaughn R. Walker

~~PROPOSED~~ ORDER

Upon consideration of the parties' joint motion for entry of an order regarding the preservation of evidence and good cause appearing, the Court hereby ENTERS the following order based on the Court's prior Order of November 6, 2007, in 06-cv-1791-VRW (Dkt. 393).

A. The Court reminds all parties of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data and tangible things in the possession, custody and control of the parties to this action, and any employees, agents, contractors, carriers, bailees or other non-parties who possess materials reasonably anticipated to be subject to discovery in this action. Counsel are under an obligation to exercise efforts to identify and notify such non-parties, including employees of corporate or institutional parties.

B. "Documents, data and tangible things" is to be interpreted broadly to include writings, records, files, correspondence, reports, memoranda, calendars, diaries, minutes, electronic messages, voicemail, e-mail, telephone message records or logs, computer and network activity logs, hard drives, backup data, removable computer storage media such as tapes, disks and cards, printouts, document image files, web pages, databases, spreadsheets, software, books, ledgers, journals, orders, invoices, bills, vouchers, checks, statements, worksheets,

1 summaries, compilations, computations, charts, diagrams, graphic presentations, drawings, films,  
2 digital or chemical process photographs, video, phonographic, tape or digital recordings or  
3 transcripts thereof, drafts, jottings and notes. Information that serves to identify, locate, or link  
4 such material, such as file inventories, file folders, indices and metadata, is also included  
5 in this definition.

6 C. "Preservation" is to be interpreted broadly to accomplish the goal of maintaining the  
7 integrity of all documents, data and tangible things reasonably anticipated to be subject to  
8 discovery under FRCP 26, 45 and 56(e) in this action. Preservation includes taking reasonable  
9 steps to prevent the partial or full destruction, alteration, testing, deletion, shredding,  
10 incineration, wiping, relocation, migration, theft, or mutation of such material, as well as  
11 negligent or intentional handling that would make material incomplete or inaccessible.

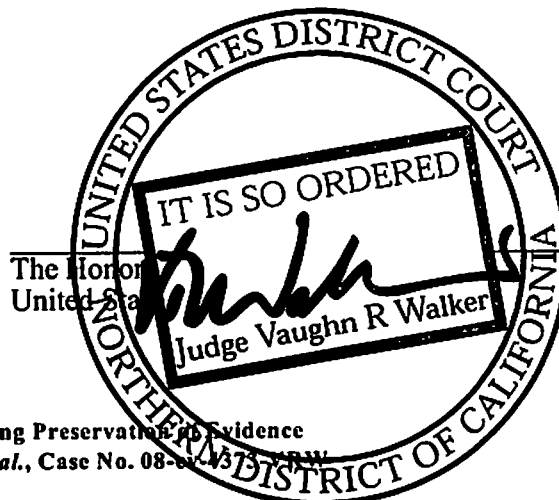
12 D. Counsel are directed to inquire of their respective clients if the business or  
13 government practices of any party involve the routine destruction, recycling, relocation, or  
14 mutation of such materials and, if so, direct the party, to the extent practicable for the pendency  
15 of this order, either to

- 16 (1) halt such business or government practices;  
17 (2) sequester or remove such material from the business or government practices; or  
18 (3) arrange for the preservation of complete and accurate duplicates or copies of such  
19 material, suitable for later discovery if requested.

20 Counsel representing each party shall, not later than December 15, 2009, submit to the  
21 Court under seal and pursuant to FRCP 11, a statement that the directive in paragraph D, above,  
22 has been carried out.

23 IT IS SO ORDERED.

24 Dated: Nov. 13, 2009.



# Exhibit D

# Exhibit D

United States District Court  
For the Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE: MDL Docket No 06-1791 VRW  
NATIONAL SECURITY AGENCY ORDER  
TELECOMMUNICATIONS RECORDS  
LITIGATION

This Document Relates To:  
ALL CASES

Plaintiffs have moved for an order prohibiting the alteration or destruction of evidence during the pendency of this action. MDL Doc # 384. The United States has filed papers opposing the motion, Doc # 386, and has prepared and lodged with the court a confidential submission designed for ex parte, in camera review. Doc # 387. Telephone company defendants AT&T, Cingular, Bellsouth, Sprint and Verizon have joined in the United States's opposition to plaintiffs' motion. Doc # 365, 388, 390.

Upon careful review of the non-confidential papers submitted in support of and in opposition to the motion, the court



1 has determined that (1) no hearing on the motion is necessary; (2)  
2 an order requiring the preservation of evidence is appropriate; and  
3 (3) an interim order shall forthwith enter requiring the parties to  
4 take steps to prevent the alteration or destruction of evidence as  
5 follows:

6           A. Until the issues in these proceedings can be further  
7 refined in light of the guidance and directives anticipated to be  
8 received upon appellate review of the court's decision in Hepting v  
9 AT&T Corporation, 439 F Supp 974 (N D Cal 2006) and of the Oregon  
10 district court's decision in Al-Haramain Islamic Foundation, Inc v  
11 Bush, 451 F Supp 2d 1215 (D Or 2006), the court reminds all parties  
12 of their duty to preserve evidence that may be relevant to this  
13 action. The duty extends to documents, data and tangible things in  
14 the possession, custody and control of the parties to this action,  
15 and any employees, agents, contractors, carriers, bailees or other  
16 non-parties who possess materials reasonably anticipated to be  
17 subject to discovery in this action. Counsel are under an  
18 obligation to exercise efforts to identify and notify such non-  
19 parties, including employees of corporate or institutional parties.

20           B. "Documents, data and tangible things" is to be  
21 interpreted broadly to include writings, records, files,  
22 correspondence, reports, memoranda, calendars, diaries, minutes,  
23 electronic messages, voicemail, e-mail, telephone message records  
24 or logs, computer and network activity logs, hard drives, backup  
25 data, removable computer storage media such as tapes, disks and  
26 cards, printouts, document image files, web pages, databases,  
27 spreadsheets, software, books, ledgers, journals, orders, invoices,  
28 bills, vouchers, checks, statements, worksheets, summaries,

1 compilations, computations, charts, diagrams, graphic  
2 presentations, drawings, films, digital or chemical process  
3 photographs, video, phonographic, tape or digital recordings or  
4 transcripts thereof, drafts, jottings and notes. Information that  
5 serves to identify, locate, or link such material, such as file  
6 inventories, file folders, indices and metadata, is also included  
7 in this definition.

8 C. "Preservation" is to be interpreted broadly to  
9 accomplish the goal of maintaining the integrity of all documents,  
10 data and tangible things reasonably anticipated to be subject to  
11 discovery under FRCP 26, 45 and 56(e) in this action. Preservation  
12 includes taking reasonable steps to prevent the partial or full  
13 destruction, alteration, testing, deletion, shredding,  
14 incineration, wiping, relocation, migration, theft, or mutation of  
15 such material, as well as negligent or intentional handling that  
16 would make material incomplete or inaccessible.

17 D. Counsel are directed to inquire of their respective  
18 clients if the business practices of any party involve the routine  
19 destruction, recycling, relocation, or mutation of such materials  
20 and, if so, direct the party, to the extent practicable for the  
21 pendency of this order, either to

22 (1) halt such business processes;

23 (2) sequester or remove such material from the business  
24 process; or

25 (3) arrange for the preservation of complete and accurate  
26 duplicates or copies of such material, suitable for later discovery  
27 if requested.


28 \\

1           The most senior lawyer or lead trial counsel representing  
2 each party shall, not later than December 14, 2007, submit to the  
3 court under seal and pursuant to FRCP 11, a statement that the  
4 directive in paragraph D, above, has been carried out.

5           The clerk is directed to vacate the hearing now scheduled  
6 for November 15, 2007 in this matter.

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

IT IS SO ORDERED.

  
\_\_\_\_\_  
VAUGHN R WALKER  
United States District Chief Judge

United States District Court  
For the Northern District of California

# Exhibit E

# Exhibit E

Cindy Cohn <Cindy@eff.org>

March 10, 2014 8:35 AM



To: "Berman, Marcia (CIV)" <Marcia.Berman@usdoj.gov>

Cc: "Gilligan, Jim (CIV)" <James.Gilligan@usdoj.gov>, "wiebe@pacbell.net"

<wiebe@pacbell.net>, Stephanie Shattuck <steph@eff.org>, "Thomas E. Moore III

(tmoore@moorelawteam.com)" <tmoore@moorelawteam.com>, "Patton, Rodney (CIV)"

<Rodney.Patton@usdoj.gov>, "Dearinger, Bryan (CIV)" <Bryan.Dearinger@usdoj.gov>, "Ilann M.

Maazel" <imaazel@ecbalaw.com>

Re: Preservation of Evidence in Jewel v. NSA and First Unitarian Church v. NSA

Security: Signed (cindy@eff.org)

Dear Marcy,

I am sorry that we did not hear from you after my message on Saturday asking for further clarification about how the government plans to ensure that it does not spoliage evidence. Unless we hear from you by noon California time today that the government does not intend to destroy evidence that may be likely to lead to the discovery of admissible evidence under the claims raised in Jewel and First Unitarian cases, we intend to seek a TRO from Judge White.

Please call or email me if you'd like to discuss this further. My cellphone is 415-307-2148. We have no desire to elevate this into an emergency matter before the court but believe we have no choice based upon the government's actions and statements so far.

Cindy

On Mar 8, 2014, at 11:43 AM, Cindy Cohn <Cindy@eff.org> wrote:

Dear Marcy,

Your response is confusing and troubling to us, as is your notice to the court in First Unitarian that you intend to begin to destroy call detail records on Tuesday, March 11, which is just two business days from now. To be clear, the only court that can relieve the government of its obligations to preserve evidence in our cases, regardless of the basis for those obligations, is the Northern District of California and it has not done so. This is true in Jewel and in First Unitarian.

As you know, both Jewel v. NSA and First Unitarian Church v. NSA arise from the ongoing bulk collection of telephone records, as did Hepting and the other MDL cases before that (along with additional information at issue in Jewel that must also be preserved). Neither the complaints nor the protective order mention the "President's Surveillance Program" so your reference to that program is confusing. The claims arise from the actual activity of bulk collection and state ongoing claims regardless of the legal or executive authority under which the government claims it conducts that activity at any point in time.

Duplicate

Cindy Cohn <Cindy@eff.org>

March 8, 2014 11:43 AM



To: "Berman, Marcia (CIV)" <Marcia.Berman@usdoj.gov>

Cc: "Gilligan, Jim (CIV)" <James.Gilligan@usdoj.gov>, "wiebe@pacbell.net" <wiebe@pacbell.net>, "Stephanie Shattuck" <steph@eff.org>, "Thomas E. Moore III (tmoore@moorelawteam.com)" <tmoore@moorelawteam.com>, "Patton, Rodney (CIV)" <Rodney.Patton@usdoj.gov>, "Dearing, Bryan (CIV)" <Bryan.Dearing@usdoj.gov>, "Ilanh M. Maazel" <imaazel@ecbalaw.com>

Re: Preservation of Evidence in Jewel v. NSA

Security:  Signed (cindy@eff.org)

Dear Marcy,

Your response is confusing and troubling to us, as is your notice to the court in First Unitarian that you intend to begin to destroy call detail records on Tuesday, March 11, which is just two business days from now. To be clear, the only court that can relieve the government of its obligations to preserve evidence in our cases, regardless of the basis for those obligations, is the Northern District of California and it has not done so. This is true in Jewel and in First Unitarian.

As you know, both Jewel v. NSA and First Unitarian Church v. NSA arise from the ongoing bulk collection of telephone records, as did Hepting and the other MDL cases before that (along with additional information at issue in Jewel that must also be preserved). Neither the complaints nor the protective order mention the "President's Surveillance Program" so your reference to that program is confusing. The claims arise from the actual activity of bulk collection and state ongoing claims regardless of the legal or executive authority under which the government claims it conducts that activity at any point in time.

Moreover, we do not understand how the preservation order in place in Jewel (and Shubert) does not also include the preservation of the records at issue in First Unitarian. We further do not understand why the government failed to inform the FISC of your duties in Jewel and Shubert since they require you to preserve the same records or why it waited until just before the deadline to seek clarity on this issue, resulting in an apparent emergency situation that could easily have been avoided.

We will seek clarification from Judge White on this but we urge you not to destroy any records relevant to our claims in either case until we can do so. Please do provide us with full information so that we can narrow the issues before the court. Frankly, your email to me yesterday and filing in the First Unitarian case yesterday raise more concerns, not less, that the government has not been fulfilling its duties to preserve relevant evidence in either case. Please note that we will seek all available remedies if it turns out that the government has not abided by its duties.

Cindy

On Mar 7, 2014, at 6:14 PM, "Berman, Marcia (CIV)" <[Marcia.Berman@usdoj.gov](mailto:Marcia.Berman@usdoj.gov)> wrote:

Cindy -- In response to your questions regarding the preservation orders in Jewel (and the prior Hepting decision), the Government's motion to the FISC, and the FISC's decision today, addressed the recent litigation challenging the FISC-authorized telephony metadata collection under Section 215 -- litigation as to which there are no preservation orders. As we indicated last week, the Government's motion did not address the pending Jewel (and Shubert) litigation because the district court had previously entered preservation orders applicable to those cases. As we also indicated, since the entry of those orders the Government has complied with our preservation obligations in those cases. At the time the preservation issue was first litigated in the MDL proceedings in 2007, the Government submitted a classified ex parte, in camera declaration addressing in detail the steps taken to meet our preservation obligations. Because the activities undertaken in connection with the President's Surveillance Program (PSP) were not declassified until December 2013, we were not able to consult with you previously about the specific preservation steps that have been taken with respect to the Jewel litigation. However, the Government described for the district court in 2007 how it was meeting its preservation obligations, including with respect to the information concerning the PSP activities declassified last December. We have been working with our clients to prepare an unclassified summary of the preservation steps described to the court in 2007 so that we can address your questions in an orderly fashion with Judge White, if you continue to believe that is necessary.

Thanks -- Marcy

---

**From:** Berman, Marcia (CIV)  
**Sent:** Friday, March 07, 2014 6:14 PM  
**To:** Cindy Cohn  
**Cc:** Gilligan, Jim (CIV); [wiebe@pacbell.net](mailto:wiebe@pacbell.net); Stephanie Shattuck; Thomas E. Moore III ([trmoore@moorelawteam.com](mailto:trmoore@moorelawteam.com)); Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel  
**Subject:** FW: Preservation of Evidence in Jewel v. NSA

Cindy -- we'll get back to you on this today, hopefully within an hour. Thanks -- Marcy

---

**From:** Dearing, Bryan (CIV)  
**Sent:** Friday, March 07, 2014 4:39 PM  
**To:** Berman, Marcia (CIV)  
**Subject:** FW: Preservation of Evidence in Jewel v. NSA

FYI ...

---

**From:** Cindy Cohn [<mailto:cindy@eff.org>]  
**Sent:** Friday, March 07, 2014 4:37 PM  
**To:** Gilligan, Jim (CIV)  
**Cc:** Rick Wiebe; Stephanie Shattuck; Thomas E. Moore III; Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel  
**Subject:** Re: Preservation of Evidence in Jewel v. NSA

Hi Jim,

I assume you've seen the FISC Order. Can you please explain how the court could be under the misimpression that there are no preservation orders for the telephone records information in place given the history at Jewel and Hepting before it? As you might expect, this is quite alarming to us.

We will be filing something shortly and I want to be sure that we correctly state your position.

Cindy

Sent from my phone

On Feb 28, 2014, at 5:17 PM, Cindy Cohn <[cindy@eff.org](mailto:cindy@eff.org)> wrote:

Hi Jim,

We'll wait a bit, assuming this doesn't drag on too long. Thanks for responding.

Cindy

Sent from my phone

On Feb 28, 2014, at 5:26 PM, "Gilligan, Jim (CIV)" <[James.Gilligan@usdoj.gov](mailto:James.Gilligan@usdoj.gov)> wrote:

Cindy,

We did receive your email about preservation, and I wanted to get back to you before the week ended to let you know that we will need a bit more time to prepare a more complete response than we will be able to do by Monday. So I would ask that you forbear from filing anything with the FISC, or Judge White, until we have further opportunity to confer. As you noted, *Jewel* and *Shubert* are not specifically mentioned in the motion we filed with the FISC, but as you also observed, the question of preservation has already been litigated in those cases, and the court issued separate preservation orders that govern there. Many of the details surrounding the intelligence programs in question remain classified, however, and so there remain limitations on our ability to confer with you concerning our compliance with those orders.

At this point I need to consult further with my clients to ascertain how much information I can convey to you about the Government's preservation efforts without revealing classified information. I simply won't be in a position to provide you with a detailed response to your



inquiry by Monday, as you request, in part because of the work that remains on our reply to your brief on the court's four questions, and in part because I will be out of the office on Monday and Tuesday for a family ski trip. (Also, as you observed, Marcy is presently diverted by another matter.) But we will do our best to address your questions by the middle of next week.

JG

James J. Gilligan  
Special Litigation Counsel  
Civil Division, Federal Programs Branch  
U.S. Department of Justice  
P.O. Box 883  
Washington, D.C. 20044

Tel: 202-514-3358

---

**From:** Cindy Cohn [<mailto:cindy@eff.org>]  
**Sent:** Friday, February 28, 2014 5:54 PM  
**To:** Gilligan, Jim (CIV)  
**Cc:** Rick Wiebe; Stephanie Shattuck; Thomas E. Moore III; Patton, Rodney (CIV); Dearing, Bryan (CIV); Ilann M. Maazel  
**Subject:** Re: Preservation of Evidence in Jewel v. NSA

Hi Jim, Rodney and Bryan,

I just wanted to confirm that you received this and learn when you will be responding.

We are planning to file something in the FISC and before Judge Walker early next week and I do want to be able to accurately convey your position.

Thanks,

Cindy

On Feb 26, 2014, at 4:08 PM, Cindy Cohn <[Cindy@eff.org](mailto:Cindy@eff.org)> wrote:

Hi Jim,

Rick will write you separately about the scheduling, but I wanted to raise something that has confused us and to seek clarification.

We saw your filing in the FISC asking that the Court's current Primary Order be amended to authorize the preservation and/or storage of call detail records beyond five years based upon your duty to preserve evidence and mentioning the First Unitarian case specifically. We do agree that the government has a duty to preserve all reasonably anticipated to be subject to discovery in this action. We were surprised, however, that you did not approach us to discuss ways that this duty could be met short of the request you made, which we read as allowing you to preserve all of the metadata you have collected.

We also write because, as I think you know, the government has been under an obligation to preserve telephone records it has collected since 2006, when the cases that made up the MDL action In Re NSA were first filed. One of those cases, Shubert v. Obama, has remained ongoing since that time. That obligation was reinforced by an Order issued by Judge Walker in 2007 and order was specifically adopted by the court in Jewel v. NSA in 2009 by a joint request by the government and the plaintiffs (Jewel v. NSA, Doc. 51).

Thus my confusion. I'm not sure why the Jewel (and Shubert) cases were not mentioned or referenced in the request to the FISC since both of those also contain ongoing preservation obligations related to the bulk phone records collection by the NSA. Since they were not, it also raises the question of whether and how the government has been abiding by its obligation to preserve evidence in those two cases, since obviously both have been pending for more than five years.

I would appreciate a prompt response and clarification. I'm confident that the government takes seriously its obligation to preserve evidence that may be relevant to pending litigation, but given the situation, I would like a specific reaffirmation that bulk telephone records collected by the NSA have been preserved in the Jewel case and I suspect Ilann is concerned about the same for Shubert. I would also request some more specific information about how that preservation has occurred -- similar to the plan you suggested to the FISC in your motion.

I hope you can provide us with a thorough response before any additional phone records are destroyed and hopefully by Monday, March 3. While we're hopeful that we will receive a satisfactory response, but if not, we do intend to raise this question with both the FISC and the Judge White.

Thanks,

Cindy

PS: Has Marcy gone? I noticed that she's not on the pleadings you filed last week or on this message.

---

Cindy Cohn  
Legal Director  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333 x108  
--- [Cindy@eff.org](mailto:Cindy@eff.org)  
--- [www.eff.org](http://www.eff.org)

Join EFF! <https://supporters.eff.org/donate>

---

Cindy Cohn  
Legal Director  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333 x108  
--- [Cindy@eff.org](mailto:Cindy@eff.org)  
--- [www.eff.org](http://www.eff.org)

Join EFF! <https://supporters.eff.org/donate>

1 CINDY COHN (SBN 145997)  
cindy@eff.org  
2 LEE TIEN (SBN 148216)  
KURT OPSAHL (SBN 191303)  
3 JAMES S. TYRE (SBN 083117)  
MARK RUMOLD (SBN 279060)  
4 ANDREW CROCKER (SBN 291596)  
ELECTRONIC FRONTIER FOUNDATION  
5 815 Eddy Street  
San Francisco, CA 94109  
6 Telephone: (415) 436-9333  
Fax: (415) 436-9993

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

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

THOMAS E. MOORE III (SBN 115107)  
tmoore@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

11  
12  
13  
14 *Counsel for Plaintiffs*

15  
16 **UNITED STATES DISTRICT COURT**  
17 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**  
18 **SAN FRANCISCO DIVISION**

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

22 Plaintiffs, )

23 v. )

24 NATIONAL SECURITY AGENCY, *et al.*, )

25 Defendants. )  
26  
27  
28

CASE NO. 08-CV-4373-JSW

**[PROPOSED] TEMPORARY  
RESTRAINING ORDER**

Hon. Jeffrey S. White  
Courtroom 11 - 19th Floor

1           This matter is before the Court on plaintiffs’ motion for a temporary restraining order to  
 2 prevent defendants National Security Agency, United States of America, Department of Justice,  
 3 Barack H. Obama, Keith B. Alexander, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their  
 4 official capacities) (collectively, the “government defendants”) and all those in active concert or  
 5 participation with them from destroying any potential evidence relevant to the claims at issue in  
 6 this action, including but not limited to prohibiting the destruction of any telephone metadata or  
 7 “call detail” records. The government defendants have given notice that they will commence  
 8 destroying call detail records on Tuesday morning, March 11, 2014. ECF No. 85 in *First*  
 9 *Unitarian Church of Los Angeles v. NSA*, No. 13-cv-3287-JSW.

10           Plaintiffs contend that the Court’s prior evidence preservation order (ECF No. 51) as well  
 11 as defendants’ obligations under the Federal Rules of Civil Procedure prohibit destruction of this  
 12 potential evidence. It is undisputed that the Court would be unable to afford effective relief to  
 13 plaintiffs once the records are destroyed, and therefore the harm plaintiffs face is irreparable. A  
 14 temporary restraining order is necessary and appropriate so that the Court may decide whether the  
 15 evidence should be preserved with the benefit of full briefing and participation by all parties.

16           It is hereby ordered that defendants National Security Agency, United States of America,  
 17 Department of Justice, Barack H. Obama, Keith B. Alexander, Eric H. Holder, Jr., and James R.  
 18 Clapper, Jr. (in their official capacities), their officers, agents, servants, employees, and attorneys,  
 19 and all those in active concert or participation with them are prohibited, enjoined, and restrained  
 20 from destroying any potential evidence relevant to the claims at issue in this action, including but  
 21 not limited to prohibiting the destruction of any telephone metadata or “call detail” records,  
 22 pending further order of the Court. The Court determines that no security is necessary under the  
 23 circumstances.

24           The Court sets the following briefing and hearing schedule in this matter:

- 25           Plaintiffs’ opening brief \_\_\_\_\_
- 26           Government defendants opposition brief \_\_\_\_\_
- 27           Plaintiffs’ reply brief \_\_\_\_\_
- 28           Hearing \_\_\_\_\_

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

This order expires at \_\_\_\_\_.

Entered at \_\_\_\_ a.m./p.m. on March \_\_\_\_, 2014

IT IS SO ORDERED.

\_\_\_\_\_

UNITED STATES DISTRICT JUDGE

United States District Court  
For the Northern District of California

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW  
No. C 13-03287 JSW

**ORDER GRANTING  
TEMPORARY RESTRAINING  
ORDER**

\_\_\_\_\_  
FIRST UNITARIAN CHURCH OF LOS  
ANGELES, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.  
\_\_\_\_\_ /

This matter is now before the Court on Plaintiffs' *ex parte* motion for a temporary restraining order requesting immediate relief. The Court **HEREBY ORDERS** that its prior evidence preservation orders in these related matters shall be enforced. It is undisputed that the Court would be unable to afford effective relief once the records are destroyed, and therefore the harm to Plaintiffs would be irreparable. A temporary restraining order is necessary and appropriate in order to allow the Court to decide whether the evidence should be preserved with the benefit of full briefing and participation by all parties.

1           Accordingly, it is HEREBY ORDERED that Defendants, their officers, agents, servants.  
2 employees, and attorneys, and all those in active concert or participation with them are  
3 prohibited, enjoined, and restrained from destroying any potential evidence relevant to the  
4 claims at issue in this action, including but not limited to prohibiting the destruction of any  
5 telephone metadata or "call detail" records, pending further order of the Court. The Court  
6 determines that there is no security necessary under the circumstances.

7           The Court sets the following briefing and hearing schedule, all in PST, in this matter:

8           Plaintiffs' opening brief shall be filed no later than March 13, 2014 at 2:00 p.m.

9           Defendants' opposition brief shall be filed no later than March 17, 2014 at 11:00 a.m.

10          Plaintiffs' reply brief shall be filed no later than March 18, 2014 at 2:00 p.m.

11          The hearing on this issue shall be set for March 19, 2014 at 2:00 p.m.

12  
13          **IT IS SO ORDERED.**

14          Dated: March 10, 2014

  
\_\_\_\_\_  
JEFFREY S. WHITE  
UNITED STATES DISTRICT JUDGE

15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28