

1 CINDY COHN (SBN 145997)  
cindy@eff.org  
2 LEE TIEN (SBN 148216)  
3 KURT OPSAHL (SBN 191303)  
4 JAMES S. TYRE (SBN 083117)  
5 MARK RUMOLD (SBN 279060)  
6 ANDREW CROCKER (SBN 291596)  
7 ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
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)  
KEKER & VAN NEST, LLP  
633 Battery Street  
San Francisco, CA 94111  
Telephone: (415) 391-5400  
Fax: (415) 397-7188

8 RICHARD R. WIEBE (SBN 121156)  
wiebe@pacbell.net  
9 LAW OFFICE OF RICHARD R. WIEBE  
10 One California Street, Suite 900  
11 San Francisco, CA 94111  
12 Telephone: (415) 433-3200  
13 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

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 )  
22 estate of GREGORY HICKS, ERIK KNUTZEN )  
23 and JOICE WALTON, on behalf of themselves )  
and all others similarly situated, )  
Plaintiffs, )  
v. )  
25 NATIONAL SECURITY AGENCY, *et al.*, )  
26 Defendants. )

Case No.: 08-cv-4373-JSW  
**PLAINTIFFS' RESPONSE TO  
DEFENDANTS' PUBLIC  
DECLARATIONS**  
Courtroom 11, 19th Floor  
The Honorable Jeffrey S. White

**TABLE OF CONTENTS**

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

INTRODUCTION..... 1

I. DEFENDANTS FAIL TO ADDRESS MANY OF THE ADMISSIONS AND UNDISPUTED PUBLIC DISCLOSURES THAT HAVE OCCURRED SINCE JUNE 2013 ..... 3

    A. Disclosures Concerning the NSA’s “Upstream” Surveillance Operations and Content Analysis of Intercepted Internet Communications ..... 3

    B. Disclosures Concerning Telecommunication Company Participation in the NSA’s Surveillance Activities ..... 6

    C. Disclosures Concerning the Ineffectiveness of the NSA’s Bulk Collection Programs ..... 8

II. ANY ADDITIONAL *EX PARTE* FILINGS IN THIS CASE SHOULD BE DECLASSIFIED AND RELEASED ..... 11

CONCLUSION ..... 13

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

**TABLE OF AUTHORITIES**

**Federal Cases**

*Hepting v. AT&T Corp.*,  
439 F. Supp. 2d 974 (N.D. Cal. 2006) .....6, 7

**Federal Statutes**

50 U.S.C. § 1806 .....1, 2, 9  
50 U.S.C. § 1881(a).....5, 8, 9

**INTRODUCTION**

1  
2 At the September 27, 2013 Case Management Conference, the Court ordered defendants to  
3 review, correct, and augment as necessary the record in this case. Transcript of Proceedings Dated  
4 September 27, 2013 (“TR”) at 8-9. In light of the recent and significant disclosures concerning the  
5 surveillance programs of the National Security Agency (“NSA”)—and in light of the effect of  
6 those disclosures on this case—the Court ordered defendants to: (1) undertake a declassification  
7 review of all materials previously submitted *ex parte*; and (2) “to file revised declarations and  
8 exhibits to accurately reflect all of the information that has now been declassified *or disclosed*.” TR  
9 at 9 (emphasis added). The Court further provided plaintiffs with an opportunity to respond to  
10 defendants’ filings. *Id.* Accordingly, plaintiffs offer this response for two reasons: first, to highlight  
11 additional information from the disclosures of the past seven months that are particularly relevant  
12 to this case, much of which defendants omit from their filings; and, second, to draw the Court’s  
13 attention to additional *ex parte* filings that defendants have not yet provided to plaintiffs.

14 There is no question that a full public accounting by the government of “all that’s been put  
15 in the . . . public domain in light of disclosures, both by government people and, also, others” (Tr.  
16 at 9) will help to narrow the issues in this case, promote judicial efficiency, minimize the need to  
17 resort to the procedures under section 1806(f), aid the Court in fashioning a result, and enhance the  
18 public perception of the integrity of the judicial process as it applies to this case. Yet, it appears to  
19 plaintiffs that the government’s public disclosures fall far short of an accurate and comprehensive  
20 presentation of all that is already in the public domain.

21 On December 20, 2013, the government filed public, redacted versions of eight declarations  
22 previously submitted *ex parte* in 2007, 2009, and 2012 in the *Jewel* and *Shubert* cases. *See* Defs.’  
23 Notice of Filing Declassified Declarations (ECF No. 172) (Attach. 1-8). Defendants also filed two  
24 new public declarations, *see* Public Declaration of James R. Clapper (“2013 Clapper Decl.”) (ECF  
25 No. 168); Unclassified Declaration of Frances J. Fleisch (“2013 Fleisch Decl.”) (ECF No. 169),  
26 and lodged two new *ex parte* declarations with the Court. Defs.’ Notice of Lodging of *In Camera*,  
27 *Ex Parte* Classified Declaration of James R. Clapper (ECF No. 170); Defs.’ Notice of Lodging of  
28 *In Camera*, *Ex Parte* Classified Declaration of Frances J. Fleisch (ECF No. 171).

1 The declassified declarations confirm that, beginning in October 2001, the NSA initiated an  
2 unprecedented set of programs of mass domestic surveillance that operated outside the scope of  
3 federal surveillance laws and the Constitution. *See* Compl., ¶¶ 2-14 (ECF No. 1); 2013 Clapper  
4 Decl., ¶¶ 5-6. These programs included the interception of the contents of communications and the  
5 bulk collection of communications records, and were initially undertaken without Court or  
6 congressional authorization. *See* 2013 Clapper Decl., ¶¶ 5-6. Defendants' filings, however, are  
7 hardly revelatory: with record evidence, plaintiffs have repeatedly described many aspects of the  
8 programs and their scope, most recently in October 2012. *See generally* Summary of Evidence  
9 ("SOE") (ECF No. 113).

10 While confirming the basic facts of plaintiffs' claims, defendants' most recent filings  
11 largely ignore or elide the unprecedented wave of disclosures giving more facts and content about  
12 the NSA's surveillance activities that have occurred over the past seven months. On a seemingly  
13 daily basis, government officials confirm new details and new documentary evidence, generally in  
14 response to information published in the nation's major media outlets. Additionally, since June,  
15 intelligence officials have publicly testified about NSA surveillance programs before Congress at  
16 least nine times; intelligence officials have made innumerable speeches and media appearances  
17 discussing NSA surveillance activities; and the Director of National Intelligence has even started  
18 its own Tumblr.com webpage to provide "immediate, ongoing and direct access to factual  
19 information" about NSA surveillance programs. *See* IC On The Record,  
20 <http://icontherecord.tumblr.com/>. The authenticity of disclosures made in news articles has either  
21 been confirmed or has not been contested by the government. It is against this backdrop that the  
22 completeness and candor of the government's December 20, 2013 disclosures to this Court must be  
23 assessed.<sup>1</sup>

24  
25  
26 <sup>1</sup> Additionally, Defendants' use of the two new Clapper and Fleisch declarations to assert the state  
27 secrets privilege is improper because the Court has already ruled that section 1806(f) displaces the  
28 state secrets privilege with respect to plaintiffs' statutory claims. Amended Order at 12-13 (ECF  
No. 153). Defendants concede that the Court's reasoning applies equally to plaintiffs'  
constitutional claims as well. Defs.' Supplemental Brief on Threshold Legal Issues at 7 (ECF  
No. 167). There is thus no basis for submission of an additional state secrets assertion.

1           Accordingly, plaintiffs offer this response to provide the Court with additional information  
2 from the disclosures of the past seven months and to draw the Court's attention to *ex parte* filings  
3 in the record that defendants, without explanation, failed to provide to plaintiffs.

4           **I.       DEFENDANTS FAIL TO ADDRESS MANY OF THE ADMISSIONS AND**  
5           **UNDISPUTED PUBLIC DISCLOSURES THAT HAVE OCCURRED SINCE**  
6           **JUNE 2013**

7           Since June 2013, a substantial amount of information about the NSA's surveillance  
8 programs has been broadly disclosed. Much of this information has been disclosed directly by the  
9 government, either on its own or in response to documents published in the press that originated  
10 with Edward Snowden. Although in some instances the government has contested inferences some  
11 have drawn from those documents, the government has never contested the authenticity of any of  
12 the Snowden documents.

13           Given the brief time available to prepare this response, plaintiffs do not attempt a  
14 comprehensive listing of all the public facts relevant to their claims that were omitted from  
15 defendants' recent filings. Instead, plaintiffs highlight public disclosures, especially those  
16 confirmed by the government or reflected in FISC decisions released by the government, that the  
17 defendants' filings fail to address relating to: (A) the NSA's so-called "upstream" collection—the  
18 interception and copying of the content of Internet communications travelling along the Internet  
19 "backbone;" (B) the participation of telecommunication providers in the NSA's domestic  
20 surveillance programs; and (C) the ineffectiveness of the NSA's bulk surveillance programs, all of  
21 which are directly relevant to this case.

22           **A.       Disclosures Concerning the NSA's "Upstream" Surveillance Operations**  
23           **and Content Analysis of Intercepted Internet Communications**

24           Plaintiffs previously submitted documentary evidence and eyewitness testimony from a  
25 former AT&T technician, Mark Klein, showing how the government, in partnership with AT&T,  
26 acquires access to the streams of international and domestic Internet communications as they flow  
27 between AT&T's Common Backbone and other carriers' networks. *See* SOE at 7. Defendants then  
28 use sophisticated surveillance equipment to search and select communications for further scrutiny

1 by human analysts. SOE at 11-13. The government has now admitted, on multiple occasions, that it  
2 engages in precisely this type of surveillance and recent disclosures provide additional details.

3 First, and most importantly, Defendants' declaration specifically mentions, albeit in  
4 passing, the NSA's "upstream collection" of Internet communications. 2013 Fleisch Decl., ¶ 29  
5 ("Second, in addition to collection directly from providers, the NSA performs 'upstream collection'  
6 of Internet communications."). Declassified portions of defendants' previous declarations further  
7 show that, in performing this type of upstream collection, defendants "search the content of"  
8 intercepted Internet communications for "targeted selectors." Classified Declaration of Frances J.  
9 Fleisch ("2012 Fleisch Decl."), ¶ 69 (ECF No. 172-8).

10 Public disclosures over the past six months, however, provide substantially more  
11 information about these collection practices than the government's passing references. In  
12 particular, the government has publicly released an opinion of the FISC confirming that "'upstream  
13 collection' refers to the acquisition of Internet communications as they transit the 'internal  
14 backbone' facilities" of telecommunications firms, such as AT&T. Mem. Op. at 26, *Redacted*,  
15 No. [Redacted] (FISC Sep. 25, 2012) (emphasis added) (Ex. 1).<sup>2</sup> Moreover, Senator Dianne  
16 Feinstein, the Chair of the Senate Select Committee on Intelligence, identically described the  
17 NSA's upstream collection process:

18 [Upstream collection] occurs when NSA obtains Internet communications, such  
19 as e-mails, from certain U.S. companies that operate the Internet backbone  
20 [*sic*]; *i.e.*, the companies that own and operate the domestic telecommunication  
lines over which Internet traffic flows.

21 Hearing on FISA legislation before the S. Select Comm. on Intelligence, 113th Cong. (Sep. 26,  
22 2013) (statement of Sen. Feinstein) (*See* Rumold Decl., ¶3). Reports by media outlets—including  
23 the *Wall Street Journal*, *New York Times*, and *Washington Post*—provide further details about  
24 defendants' upstream collection. For example, the *Wall Street Journal* reported:

25 The NSA asks telecom companies to send it various streams of Internet traffic it  
26 believes most likely to contain foreign intelligence. This is the first cut of the  
27 data. . . The second cut is done by NSA. It briefly copies the traffic and decides  
which communications to keep based on what it calls "strong selectors"—say, an

28 <sup>2</sup> All exhibit numbers cited herein refer to the documents attached to the Declaration of Mark  
Rumold, which accompanies this filing.

1 email address, or a large block of computer addresses that correspond to an  
2 organization it is interested in . . . The system is built with gear made by Boeing  
3 Co.'s Narus subsidiary, which makes filtering technology, and Internet hardware  
4 manufacturers Cisco Systems Inc. and Juniper Networks Inc[.]

5 Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance*  
6 *Reach*, Wall. St. J. (Aug. 20, 2013) (Ex. 2); *see also* Joint Statement From the Office of the  
7 Director of National Intelligence and the National Security Agency (Aug. 21, 2013) (“Aug. 21  
8 Joint Statement”) (Ex. 3) (confirming, in response to the *Wall Street Journal* article, that the  
9 “assistance from the providers . . . is the same activity that has been previously revealed as part of  
10 Section 702 collection and PRISM”). These descriptions of upstream Internet surveillance are  
11 functionally identical to the surveillance configuration described by the Klein evidence: a system  
12 designed to acquire Internet communications as they flow between AT&T’s Common Backbone  
13 Internet network to the networks of other providers. *See* SOE at 6-9.

14 Government documents and media accounts also confirm that defendants search the  
15 content of communications acquired through “upstream collection” after the communications are  
16 intercepted. As noted in an October 2011 opinion of the Foreign Intelligence Surveillance Court,  
17 the government not only intercepts communications “to” and “from” surveillance targets, but also  
18 engages in widespread content searches for communications “about” a surveillance target. *See*  
19 *Mem. Op., Redacted*, 2011 WL 10945618 at \*6 n.16 (FISC Oct. 3, 2011). “[A]ll ‘about’  
20 communications”—that is, communications containing a “targeted selector”—“are acquired by  
21 means of NSA’s acquisition of Internet transactions through its upstream collection.” *Id.* A draft  
22 report by the NSA’s Office of Inspector General (the authenticity of which the government has not  
23 disputed) explains that “[f]or Internet content selectors, collection managers [at NSA] sent tasking  
24 instructions directly to equipment installed at company-controlled locations.” Office of Inspector  
25 General, National Security Agency (“Draft OIG Report”) (March 24, 2009) at 17 (ECF No. 147  
26 Ex. A);<sup>3</sup> *see also* Charlie Savage, *NSA Said to Search Content of Messages To and From U.S.*,  
27 *N.Y. Times* (Aug. 8, 2013) (Ex. 4) (By making a “clone of selected communication links,” “the  
28 N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-

<sup>3</sup> Available at <http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection>



1 mails and other text-based communications that cross the border.”). Targeting procedures,  
2 employed by defendants in 2009, confirm that:

3 in those cases where NSA seeks to acquire communications about the target that  
4 are not to or from the target, NSA will either employ an Internet Protocol filter to  
5 ensure that the person from whom it seeks to obtain foreign intelligence  
6 information is located overseas, or it will target Internet links that terminate in a  
7 foreign country.

8 *Procedures Used by the National Security Agency for Targeting Non-United States Persons* (2009)  
9 (Ex 5). These procedures thus describe a system wherein defendants intercept the stream of  
10 Internet communications, filter those communications based on IP address, then search the content  
11 of those communications—including communications of American citizens—for information  
12 “about” a surveillance target.

13 In sum, substantial information has been disclosed concerning the scope and operation of  
14 the NSA’s surveillance activities that is directly relevant and material to plaintiffs’ claims in this  
15 case.

16 **B. Disclosures Concerning Telecommunication Company Participation in  
17 the NSA’s Surveillance Activities**

18 In addition to information concerning the scope and operational details of NSA  
19 surveillance, the past seven months have resulted in the disclosure of additional information  
20 describing telecommunication company participation in the NSA’s surveillance programs.

21 Plaintiffs have alleged from the outset that the NSA’s domestic surveillance operations  
22 function “in concert with major [American] telecommunications companies,” such as AT&T and  
23 Verizon. *See* Compl. ¶¶ 2, 8-10. The fact that AT&T facilitates the government’s surveillance at  
24 issue in this case is long settled: even prior to the disclosures of the past seven months, eyewitness  
25 testimony, documentary evidence, and extensive media coverage amply demonstrated that AT&T  
26 facilitates the NSA’s surveillance of domestic and international communications and  
27 communications records. *See* SOE 25-28. Even on the limited public record that existed eight years  
28 ago, Judge Walker in *Hepting* (a related predecessor to this case) concluded that “AT&T and the  
government have for all practical purposes already disclosed that AT&T assists the government in

1 monitoring communication content.” *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 991-92 (N.D.  
2 Cal. 2006). The recent public disclosures only further confirm this long-standing conclusion.

3           Nevertheless, defendants claim ongoing national security harm from the disclosure of any  
4 “information that may tend to confirm or deny whether AT&T, Verizon, or to the extent necessary,  
5 any other particular telecommunications providers, has assisted any NSA intelligence activity,  
6 including but not necessarily limited to the alleged intelligence activities.” 2013 Clapper Decl.,  
7 ¶ 42. Such a demonstrably overbroad assertion cannot be sustained, and in fact was specifically  
8 rejected by Judge Walker in 2007. *Hepting*, 439 F. Supp. 2d at 993 (“AT&T’s assistance in  
9 national security surveillance is hardly the kind of ‘secret’ . . . that a potential terrorist would fail to  
10 anticipate”). The Court rejected the government’s position that any confirmation of AT&T’s  
11 participation in the same activities alleged here would harm national security, holding that “public  
12 disclosures by the government and AT&T indicate that AT&T is assisting the government to  
13 implement some kind of surveillance program” and, accordingly, “[b]ecause of the public  
14 disclosures by the government and AT&T, the court cannot conclude that merely maintaining this  
15 action creates a ‘reasonable danger’ of harming national security.” *Id.* at 994.

16           Recent disclosures provide only further confirmation: the NSA Draft OIG Report describes  
17 in detail the NSA’s relationship with two private sector companies described as “Company A” and  
18 “Company B” in the report. *See* Draft OIG Report at 27, 33-34. Only Companies A and B  
19 participated in all facets of the NSA’s domestic surveillance operation—the interception of both  
20 telephony and Internet content and metadata—from the inception of the NSA’s surveillance  
21 program. *Id.* at 33-34. The NSA’s relationship with these two companies was among NSA’s “most  
22 productive,” enabling NSA access to large volumes of communications “transiting the United  
23 States through fiber-optic cables, gateway switches, and data networks.” *Id.* at 28-29. Company A  
24 and Company B were the two largest providers of international telephone calls into and out of the  
25 United States. *See id.* at 27. FCC records confirm that AT&T and Verizon (formerly  
26 MCI/Worldcom) were the country’s two largest international providers at that time. Wireline  
27 Competition Bureau, FCC, 2001 International Telecommunications Data at 33 fig. 9 (Dec. 2000).<sup>4</sup>

28 \_\_\_\_\_  
<sup>4</sup> *Available at:*

Case No. C-08-4373-JSW

1 Defendants have also confirmed company participation in NSA surveillance activities in  
2 response to media reports that describe the involvement of electronic communications service  
3 providers—like Google, Microsoft, and Facebook—as well as telecommunication service  
4 providers—like AT&T and Verizon. *See, e.g.*, Director of National Intelligence, Facts on the  
5 Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act  
6 (June 8, 2013) (Ex. 6) (addressing PRISM disclosures); *see also* Aug. 21 Joint Statement  
7 (addressing Gorman & Valentino-Devries, *New Details Show Broader NSA Surveillance Reach*,  
8 Wall. St. J., *supra* at 5, describing participation of AT&T and Verizon in NSA operations).

9 Accordingly, and despite the government’s claims to the contrary, the fact that  
10 telecommunications companies—including AT&T and Verizon—have participated in the NSA’s  
11 surveillance activities is hardly a secret. Indeed, their claims of secrecy have been rejected by the  
12 Court since 2007.

13 **C. Disclosures Concerning the Ineffectiveness of the NSA’s Bulk Collection**  
14 **Programs**

15 The public debate on the propriety of the NSA’s surveillance programs has also included  
16 significant public scrutiny and disclosures concerning the efficacy—and lack thereof—of the  
17 NSA’s bulk collection programs in guarding our nation’s security. The disclosures have shown  
18 that, despite repeated government claims to the contrary, the bulk collection of communications  
19 has produced little intelligence of value and has played almost no role in preventing terrorist  
20 attacks. In its filings in with this Court, the government appears to have renewed the claims of  
21 efficacy that have been rejected—and that it has abandoned—elsewhere.

22 The government’s previous *ex parte* declarations claimed bulk collection was “an essential  
23 tool” that provided “vital ongoing intelligence.” Classified Decl. of J. Michael McConnell (“2007  
24 McConnell Decl.”), ¶ 49(3), (4) (ECF No. 172-1). Similarly, General Alexander claimed: “The  
25 bulk metadata collection activities that have ben undertaken by the NSA since 9/11 are vital tools  
26 for protecting the United States from another catastrophic terrorist attack.” Classified Decl. of  
27 Lt. Gen. Keith Alexander (“2009 Alexander Decl.”), ¶ 50; ¶ 55 (NSA’s bulk collection programs  
28 have “provided 277 reports to the FBI. These reports have tipped a total of 2,900 telephone

1 identifiers as being in contact with identifiers associated with [redacted]”); *see also* Classified  
2 Decl. of Lt. Gen. Keith B. Alexander (“2007 Alexander Decl.”), ¶¶ 58-61 (172-2). Indeed, the  
3 government continues to assert the bulk collection programs constitute “important and vital  
4 ongoing intelligence operations,” 2013 Clapper Decl., ¶ 41, that are “essential to our ability to  
5 identify the enemy and to detect and disrupt its plans for further attacks on the United States.”  
6 Fleisch Decl., ¶ 17.

7 However, public scrutiny of these claims has undermined their credibility, and the  
8 government has been forced in other contexts to admit this. For example, at a Senate Intelligence  
9 Committee hearing in September the government claimed the NSA’s bulk records collection  
10 program had lead to “understanding and disrupting 54 terror-related events.”<sup>5</sup> However, in later  
11 questioning before the Senate Judiciary Committee, General Alexander was forced to admit,  
12 despite the government’s previous claims, that the records collection program had only provided  
13 useful intelligence in one or two instances:

14 SEN. LEAHY: [W]e’ve heard over and over again the assertion that 54 terrorist plots  
15 were thwarted by the use of Section 215 and-or Section 702 authorities. That’s plainly  
16 wrong, but we still get it in letters to members of Congress, we get it in statements.  
17 These weren’t all plots and they weren’t all thwarted. The American people are getting  
18 left with the inaccurate impression of the effectiveness of NSA programs.

19 Would you agree that the 54 cases that keep getting cited by the administration were not  
20 all plots, and of the 54, only 13 had some nexus to the U.S., would you agree with that,  
21 yes or no?

22 GEN. ALEXANDER: Yes.

23 SEN. LEAHY: OK. At our last hearing, Deputy Director Inglis’ testimony stated that  
24 there’s only really one example of a case where but-for the use of Section 215, both  
25 phone records collection, terrorist activity was stopped. Is Mr. Inglis right?

26 GEN. ALEXANDER: He’s right. I believe he said two, Chairman. I may have that  
27 wrong, but I think he said two. And I would like to point out that it could only have  
28 applied in 13 of the cases, because of the 54 terrorist plots or events, only 13 occurred in  
the U.S. Business record FISA was only used in 12 ...

SEN. LEAHY: I understand that, but what I worry about is ... we have these  
overstatements of what’s going on. We’re talking about massive, massive, massive

<sup>5</sup> Hearing on FISA legislation before the S. Select Comm. on Intelligence, 113th Cong. (Sep. 26, 2013) (Statement of Gen. Alexander) (*See* Rumold Decl., ¶9).

1 collection. We're told we have to do that to protect us, and then statistics are rolled out.  
2 If they are not accurate, it doesn't help with the credibility here in the Congress, doesn't  
3 help the credibility with this chairman, and doesn't help with the credibility with the  
4 country.

5 Hearing on FISA oversight before the S. Comm. on the Judiciary, 113th Cong. (Oct 2, 2013) (*See*  
6 Rumold Decl., ¶ 10). And, even in those two cases, the bulk collection of communications records  
7 was unnecessary: as Senators Heinrich, Udall, and Wyden, all members of the Senate Select  
8 Committee on Intelligence have stated, "the government could have used its more targeted  
9 authorities to obtain the phone records it claims were valuable" in those cases. Brief of Amici  
10 Curiae Senator Ron Wyden, Senator Mark Udall & Senator Martin Heinrich at 11-13, *First*  
11 *Unitarian Church, et al. v. NSA, et al.*, No. 3:13-cv-03287 JSW (N.D. Cal. Nov. 18, 2013) (ECF  
12 No. 63). The independent review group appointed by President Obama to review the NSA's  
13 surveillance programs agreed. The group found the bulk collection of calling information "was not  
14 essential to preventing attacks and [any useful information] could readily have been obtained in a  
15 timely manner" using a targeted approach. President's Review Grp. on Intelligence and Commc'ns  
16 Tech., *Liberty and Security in a Changing World* at 104 (Dec. 12, 2013) (Ex. 7).

17 To provide one additional example of the government's exaggerated claims, defendants  
18 regularly cite the intelligence community's failure to catch Khalid al-Mihdhar, one of the 9/11  
19 hijackers, as a justification for the bulk collection of communications. *See, e.g.*, Declaration of  
20 Teresa B. Shea, ¶ 11, *First Unitarian Church*, No. No. 3:13-cv-03287 JSW (ECF No. 67-1)  
21 ("Telephony metadata of the type acquired under this program . . . might have permitted NSA  
22 intelligence analysts to tip FBI to the fact that al-Mihdhar was [in the U.S.]"); Hearing on  
23 disclosure of National Security Agency Surveillance Programs before the H. Permanent Select  
24 Comm. on Intelligence, 113th Cong. (Jun. 18, 2013) (testimony of Gen. Keith Alexander) (*see*  
25 Rumold Decl., ¶12) ("We couldn't connect the dots because we didn't have the dots."); *see also*  
26 2007 Alexander Decl., ¶ 58 (stating the existence of the government's "meta data activities would  
27 have provided a highly significant tool that may have proved valuable in detecting the 9/11 plot.").  
28 Al-Mihdhar lived in San Diego for a year and a half prior to the September 11th attacks, and the  
intelligence community intercepted his conversations with a terrorist safe house in Yemen. Peter  
Bergen, *Would NSA Surveillance Have Stopped 9/11 Plot?*, CNN (Dec. 30, 2013) (Ex. 8).

1           However, the government’s claim that it was the absence of a bulk communications  
2 collection program that prevented detection of al-Mihdhar has been thoroughly discredited. To the  
3 contrary, it was the intelligence community’s failure to share and act on information *it had already*  
4 *acquired* that resulted in al-Mihdhar escaping scrutiny. *Id.* (“The government missed multiple  
5 opportunities to catch al Qaeda hijacker Khalid al-Mihdhar . . . not because it lacked access to all  
6 Americans phone records but because it didn’t share the information it already possessed about the  
7 soon-to-be-hijacker within other branches of government.”); *see also* Justin Elliot, *Judge on NSA*  
8 *Case Cites 9/11 Report, But It Doesn’t Actually Support His Ruling*, ProPublica (Dec. 28, 2013)  
9 (noting “experts say the NSA could have avoided the pre-9/11 failure even without the metadata  
10 surveillance program”) (Ex. 9); Michael German, *No NSA Poster Child: The Real Story of 9/11*  
11 *Hijacker Khalid al-Mihdhar*, Defense One (Oct. 16, 2013) (Ex. 10).

12           In sum, the government’s declarations in this case have provided the Court with an  
13 incomplete picture—both of the NSA’s surveillance programs and the degree to which those  
14 programs have been publicly disclosed. Substantial governmental admissions and other  
15 uncontroverted information exist concerning the scope and operational details of the NSA’s  
16 programs, the telecommunication carriers’ participation in those programs, and the efficacy of the  
17 programs.

## 18           **II. ANY ADDITIONAL *EX PARTE* FILINGS IN THIS CASE SHOULD BE** 19           **DECLASSIFIED AND RELEASED**

20           Despite the governments’ public filings, and despite plaintiffs’ best attempt to augment the  
21 gaps in those filings, the record in this case is still incomplete: there are additional *ex parte* filings  
22 in this case that have not yet been publicly released, even in redacted form.

23           The Court ordered the government to perform a declassification review of “[a]ny materials  
24 already submitted *ex parte* by defendants.” TR at 8-9 (emphasis added). Yet review of the public  
25 docket, and the governments’ recent filings, demonstrates that additional materials have yet to be  
26 provided to plaintiffs.<sup>6</sup>

27           <sup>6</sup> In fact, defendants’ filing of two additional *ex parte* declarations only adds to the collection of  
28 materials to which plaintiffs have been unnecessarily denied access. *See* Defs.’ Notice of Lodging  
of *In Camera, Ex Parte* Classified Declarations (ECF Nos. 170, 172). Both those declarations, too,  
Case No. C-08-4373-JSW

1 For example, the Fleisch Declaration indicates that two sets of *ex parte* declarations were  
2 filed in *Jewel* and *Shubert* in September and November 2012. *See* 2013 Fleisch Decl., ¶ 19 (“I am  
3 familiar with the previous classified declarations filed in these cases in September and November  
4 2012”). The government has only made available the declarations filed in September 2012. *See*  
5 2012 Clapper Decl., (dated September 11, 2012); 2012 Fleisch Decl., (dated September 11, 2012).  
6 The government offers no explanation for this apparent discrepancy.

7 To provide another example, the 2007 Alexander Declaration notes that “the United States  
8 notified this court on April 9, 2007” that one FISA Court judge had rejected orders issued by a  
9 previous FISA Court judge. *See* 2007 Alexander Decl., ¶ 26. The April 9, 2007 notification  
10 concerned the “Domestic Content Order” and “Foreign Content Order,” originally issued by the  
11 FISC on January 10, 2007. 2007 Alexander Decl., ¶ 26; Draft OIG Report at 40-42. These orders  
12 shifted the NSA’s content collection program, previously operating only under Presidential  
13 authorization, to the supervision of the FISC. *See* 2007 Alexander Decl., ¶ 26. However, in  
14 April 2007, another FISC judge determined the program to be unlawful and substantially altered  
15 the original orders. *See id.*; *see also* SOE at 39-40. The government has not made the April 9, 2007  
16 notification available to plaintiff, nor has it provided any reason that it should remain secret.<sup>7</sup>  
17 Given that the claims in this suit relate precisely to the collection of domestic communications  
18 content, given that the FISC apparently determined the domestic content collection was unlawful,  
19 and in the absence of a legitimate justification, the government’s bald attempt to shield this  
20 information from disclosure should not be countenanced. Indeed, to the extent the government has  
21 lodged any decision of the FISC with this Court, those decisions must be disclosed.

22 Other examples of unaccounted-for *ex parte* filings include:

- 23 • *Ex Parte* Supplemental Memorandum of Government Defendants in Support of Motion to  
24 Dismiss and for Summary Judgment (Apr. 3, 2009) (ECF No. 21);

25 should be provided in redacted form, and plaintiffs respectfully request the Court order the  
26 government to provide plaintiffs with redacted versions of all future *ex parte* filings.

27 <sup>7</sup> The government has also redacted all references to the Domestic Content Order from the publicly  
28 released declarations. *See, e.g.*, Classified Decl. of Dennis C. Blair, ¶ 41 (ECF No. 172-3);  
Classified Decl. of Deborah A. Bonanni, ¶ 64 (ECF No. 172-5).

- 1 • United States' Classified *In Camera, Ex Parte* Supplemental Memorandum in Opposition
- 2 to Plaintiffs' Motion for an Order to Preserve Evidence (filed in *Shubert*) (Oct. 25, 2007)
- 3 (ECF No. 20);
- 4 • Classified *In Camera, Ex Parte* Declaration of a Senior NSA Official (filed in *Shubert*)
- 5 (October 25, 2007) (ECF No. 20); and
- 6 • Classified *In Camera, Ex Parte* Supplemental Memorandum of Points and Authorities
- 7 (filed in *Shubert*) (Oct. 30, 2009) (ECF No. 41).

8 Defendants offer no reason for failing to comply with the Court's order to provide these documents  
 9 in redacted form. Consistent with the Court's prior order, to the extent *any* documents have been  
 10 filed *ex parte* with the Court, those documents, too, should be declassified and released.

### 11 CONCLUSION

12 Defendants' surveillance programs are no secret. Substantial admissions and other  
 13 information exist in the public domain for this Court to adjudicate the lawfulness of the  
 14 government's programs without risking harm to national security. The disclosures of the past seven  
 15 months—as described in summary fashion above—amply demonstrate that fact. However, without  
 16 full and complete access to materials in the record, the quick, effective, and reasonable resolution  
 17 of this case will suffer. Plaintiffs respectfully request the Court order the government to remedy the  
 18 deficiencies described above.

19 DATE: January 10, 2014

Respectfully submitted,

20 \_\_\_\_\_  
 21 /s/ Cindy Cohn

22 CINDY COHN  
 23 LEE TIEN  
 24 KURT OPSAHL  
 25 JAMES S. TYRE  
 26 MARK RUMOLD  
 27 ANDREW CROCKER  
 28 ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE  
 LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III  
 ROYSE LAW FIRM, PC



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

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

ARAM ANTARAMIAN  
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs