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

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

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

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

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 08-cv-4373-JSW

PLAINTIFFS' RESPONSE TO DEFENDANTS' PUBLIC DECLARATIONS

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

INTRODUCTION

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

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

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

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

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

[1] Additionally, Defendants' use of the two new Clapper and Fleisch declarations to assert the state secrets privilege is improper because the Court has already ruled that section 1806(f) displaces the 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.

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

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

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

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

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

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

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

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

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

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

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

> The NSA asks telecom companies to send it various streams of Internet traffic it believes most likely to contain foreign intelligence. This is the first cut of the 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

[2] All exhibit numbers cited herein refer to the documents attached to the Declaration of Mark Rumold, which accompanies this filing.

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

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

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

[3] *Available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection

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

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

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

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

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

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

Plaintiffs have alleged from the outset that the NSA's domestic surveillance operations function "in concert with major [American] telecommunications companies," such as AT&T and Verizon. *See* Compl. ¶¶ 2, 8-10. The fact that AT&T facilitates the government's surveillance at issue in this case is long settled: even prior to the disclosures of the past seven months, eyewitness testimony, documentary evidence, and extensive media coverage amply demonstrated that AT&T facilitates the NSA's surveillance of domestic and international communications and communications records. *See* SOE 25-28. Even on the limited public record that existed eight years 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

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

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

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

[4] *Available at*:

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

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

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

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

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

http://transition.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/Intl/4361-f99.pdf.

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

However, public scrutiny of these claims has undermined their credibility, and the government has been forced in other contexts to admit this. For example, at a Senate Intelligence Committee hearing in September the government claimed the NSA's bulk records collection program had lead to "understanding and disrupting 54 terror-related events."[5] However, in later questioning before the Senate Judiciary Committee, General Alexander was forced to admit, despite the government's previous claims, that the records collection program had only provided useful intelligence in one or two instances:

> SEN. LEAHY: [W]e've heard over and over again the assertion that 54 terrorist plots were thwarted by the use of Section 215 and-or Section 702 authorities. That's plainly wrong, but we still get it in letters to members of Congress, we get it in statements. These weren't all plots and they weren't all thwarted. The American people are getting left with the inaccurate impression of the effectiveness of NSA programs.
>
> Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and of the 54, only 13 had some nexus to the U.S., would you agree with that, yes or no?
>
> GEN. ALEXANDER: Yes.
>
> SEN. LEAHY: OK. At our last hearing, Deputy Director Inglis' testimony stated that there's only really one example of a case where but-for the use of Section 215, both phone records collection, terrorist activity was stopped. Is Mr. Inglis right?
>
> GEN. ALEXANDER: He's right. I believe he said two, Chairman. I may have that wrong, but I think he said two. And I would like to point out that it could only have 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

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

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

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

To provide one additional example of the government's exaggerated claims, defendants regularly cite the intelligence community's failure to catch Khalid al-Mihdhar, one of the 9/11 hijackers, as a justification for the bulk collection of communications. *See, e.g.*, Declaration of Teresa B. Shea, ¶ 11, *First Unitarian Church*, No. No. 3:13-cv-03287 JSW (ECF No. 67-1) ("Telephony metadata of the type acquired under this program . . . might have permitted NSA intelligence analysts to tip FBI to the fact that al-Mihdhar was [in the U.S.]"); Hearing on disclosure of National Security Agency Surveillance Programs before the H. Permanent Select Comm. on Intelligence, 113th Cong. (Jun. 18, 2013) (testimony of Gen. Keith Alexander) (*see* Rumold Decl., ¶12) ("We couldn't connect the dots because we didn't have the dots."); *see also* 2007 Alexander Decl., ¶ 58 (stating the existence of the government's "meta data activities would have provided a highly significant tool that may have proved valuable in detecting the 9/11 plot."). 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).

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

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

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

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

The Court ordered the government to perform a declassification review of "[*a*]*ny* materials already submitted *ex parte* by defendants." TR at 8-9 (emphasis added). Yet review of the public docket, and the governments' recent filings, demonstrates that additional materials have yet to be provided to plaintiffs.[6]

[6] In fact, defendants' filing of two additional *ex parte* declarations only adds to the collection of 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,

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

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

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

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

---

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

[7] The government has also redacted all references to the Domestic Content Order from the publicly 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).

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

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

CONCLUSION

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

DATE: January 10, 2014

Respectfully submitted,

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

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
ROYSE LAW FIRM, PC

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