STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358; Fax: (202) 616-8470
Attorneys for the Government Defs. in their Official Capacity

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. 3:08-cv-04373-JSW Case No. 3:13-cv-03287-JSW **GOVERNMENT DEFENDANTS' RESPONSE TO PLAINTIFFS' OPENING BRIEF RE: PRESERVATION** Date: March 19, 2014 Time: 2:00 p.m. Courtroom 11, 19th Floor The Honorable Jeffrey S. White
FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	

INTRODUCTION

The instant matter puts the Government between two competing legal obligations—the asserted requirement to preserve data that Plaintiffs contend are relevant to this litigation, and the Government's obligation to comply with orders of the Foreign Intelligence Surveillance Court ("FISC") that require the Government to destroy those same data in accordance with provisions of the Foreign Intelligence Surveillance Act ("FISA"). The Government takes both obligations seriously, but cannot comply with both. Resolution of the conflict first requires this Court to determine whether Plaintiffs have shown that access to these data would be sufficiently relevant and beneficial to their case to justify the burdens that preservation of the data would entail. Plaintiffs' central contention, that the preservation order entered in *Jewel* already requires preservation of the data at issue, is plainly in error, and based on a wholesale rewriting of the allegations in that case, which unambiguously challenge intelligence activities carried out under *Presidential*, not FISC, authorization.

In contrast, Plaintiffs in *First Unitarian* and a number of other civil actions pending in district courts around the country contest the legality of the NSA's bulk collection of telephony metadata. Pursuant to a provision of FISA known as Section 215 the NSA collects bulk in "telephony metadata" (also known as call detail records) from certain telecommunications service providers, business records that contain such information as the time and duration of calls made, and the numbers dialed, but not the content of anyone's communications. Collection of these records, which has been repeatedly authorized by the FISC as consistent with governing law, and constitutional, permits NSA analysts to detect communications between foreign terrorists and any contacts of theirs located in the United States.

As required by FISA, the FISC's orders authorizing the NSA telephony metadata program impose strict requirements, known as minimization procedures, limiting access to and dissemination of the data to valid counter-terrorism purposes. Among these is a requirement that the data be destroyed within five years after they are collected, to protect the privacy interests of U.S. persons. As this Court is aware, the Government recently moved the FISC for leave to preserve certain metadata that are currently subject to this destruction requirement, in recognition

that the data may be deemed relevant to the plaintiffs' cases in the various suits challenging the program's lawfulness. On March 7, 2014, the FISC denied that request without prejudice, finding that preservation would be inconsistent with FISA's minimization requirements, at least on the record then before the court. However, following this Court's March 10 order directing that the data be preserved pending further instruction from this Court, the FISC on March 12, 2014, granted the Government leave to retain the data pending resolution of the instant matter, in recognition that it is now necessary and appropriate for this Court to determine whether preservation of the data is required for purposes of this litigation.

In their opening brief ("Pls.' Br."), Plaintiffs primarily contend that the question at hand was already litigated and decided in *Jewel*. But *Jewel* (as well as the pending companion case, *Shubert v. Obama*) plainly concerns alleged surveillance activities undertaken pursuant to presidential authorization, *i.e.*, *without* judicial authorization under FISA. In 2007 the Government detailed for the Court the preservation efforts it had undertaken regarding those presidentially authorized activities, and Plaintiffs fail entirely to demonstrate that the Government's preservation obligations in *Jewel* extend to FISC-authorized activities.

Specifically, the Government has preserved a wide range of documents and information related to the intelligence activities authorized by President Bush after the 9/11 terrorist attacks—that is, the Terrorist Surveillance Program (TSP), under which international communications to or from the United States reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization were intercepted, and the bulk collection of Internet and telephony metadata. The Government has preserved this information because it is potentially relevant to the plaintiffs' claims in *Jewel* (and *Shubert*) that following the 9/11 attacks, President Bush authorized the NSA to undertake, with the assistance of major telecommunications companies, indiscriminate surveillance of the content of communications and communications records of millions of Americans without court approval.

The Government's preservation obligations in *Jewel* do not, however, extend to the preservation of information acquired under FISC orders, because the lynchpin of the claims in *Jewel* (and *Shubert*) is that the challenged activity occurred without court approval. Indeed, at

the time the question of preservation was first litigated in the related multi-district litigation in 2007, the Government specifically informed the Court of this limitation on the scope of potentially relevant evidence in a detailed classified filing before the Court entered its preservation order.[1] Thus, far from "conced[ing]" that information collected pursuant to FISC orders is relevant in *Jewel* and *Shubert*, as Plaintiffs contend, the Government has consistently hewed to its understanding of the *Jewel* Plaintiffs' claims as challenging presidentially-authorized activity that occurred without court approval.

Other than to place reliance on the preservation order in *Jewel*, Plaintiffs say little to explain why preservation of telephony metadata that the NSA would otherwise age off in compliance with the FISC's five-year retention limit is required under the circumstances even of the *First Unitarian* case, which expressly challenges the FISC-authorized telephony metadata program. As the Government acknowledged before the FISC and does so again here, the data at issue are potentially relevant to the claims in cases, such as *First Unitarian*, involving challenges to the FISC-authorized telephony metadata program. That is why the Government initially sought leave from the FISC to preserve them. But, particularly in light of the FISC's March 7 ruling, the question now is whether Plaintiffs can show that the potential value to this litigation of retaining the data outweighs the burdens of doing so.

A court considering a party's request for preservation of information must balance the burden on the non-movant of preserving the information at issue against with the moving party's demonstration of the information's potential benefit to its case. As discussed below, preservation of the data in question would place substantial burdens on the NSA and require a significant diversion of financial, technological, and personnel resources from accomplishment of the agency's core national security mission. In addition, mass preservation of telephony metadata that the NSA would otherwise age off would contravene the important public policies and privacy interests that underlie FISA's minimization requirements. For their part, Plaintiffs do not explain why preservation of these data is necessary in order to litigate their standing to challenge the telephony metadata program in *First Unitarian* when, assuming *arguendo* that data

[1] A redacted, unclassified version of that declaration is filed herewith.

pertaining to Plaintiffs' phone calls was collected at all, the NSA would continue to retain a much larger body of data for purposes of ongoing intelligence activities. Nevertheless, if this Court determines that the data, collected under authority of FISA, should be preserved in contravention of FISA's minimization requirements, then the Government will seek leave from the FISC to preserve the records, and will abide by the courts' ultimate determination of where the Government's legal obligations lie.

The remaining issues raised by Plaintiffs require little discussion. The Government has no objection to the entry of a preservation order in *First Unitarian* such as that entered in *Jewel*, so long as the Government's obligations regarding preservation of telephony metadata are made clear and the Government is not left in the position of having to comply with conflicting court orders regarding the preservation (or destruction) of telephony metadata that are subject to the FISC's five-year retention limit. So far as Plaintiffs' request for disclosure of the Government's preservation efforts is concerned, submitted herewith is a declassified NSA declaration, originally filed in related multi-district litigation in 2007, that details the steps the Government has taken to preserve documents and information pertaining to the NSA's prior collection of telephony metadata, Internet metadata, and communications content under Presidential authority in the wake of the September 11, 2001, terrorist attacks. While it was not possible to prepare an equally detailed response regarding NSA's collection of communications metadata and content under FISC authorization under the current briefing schedule, the Government is prepared to submit a detailed explanation of those preservation efforts should the Court desire.

BACKGROUND

A. Prior Preservation Orders in *Jewel* and *Shubert* in MDL-1791

In assessing the preservation obligations applicable in *Jewel* and *Shubert*, and in *First Unitarian*, the respective background – and differences in the claims raised in these cases – must first be set forth. As detailed further below, while Plaintiffs in *First Unitarian* clearly challenge the bulk collection of telephony metadata authorized by the FISC under Section 215, Plaintiffs in both the *Jewel* and *Shubert* litigation unambiguously challenged alleged surveillance activities authorized by the President after the 9/11 attacks specifically and repeatedly on the grounds that

these activities were undertaken without judicial approval and outside of the requirements of statutory law, including the FISA.

In *Jewel* and *Shubert*, Plaintiffs claim "that the federal government, with the assistance of major telecommunications companies, conducted widespread warrantless dragnet communications surveillance of United States citizens following the attacks of September 11, 2001." *Jewel v. NSA*, --- F. Supp. 2d ---, 2013 WL 3829405, at * 2 (N.D. Cal. July 23, 2013). Of the two cases, *Shubert* was filed first, on May 17, 2006, and it was transferred to the *In re NSA Telecommunications Records Litigation* Multi-District Litigation (MDL) proceeding (designated as 3:06-md-1791-VRW (hereafter MDL-1791)). Joint Case Management Statement at 24 (ECF No. 159).[2] The *Jewel* complaint was filed on Sept. 18, 2008. *Id*. at 1. On Plaintiffs' motion, *Jewel* was related to *Hepting v. AT&T*, No. 06-cv-0672 (N.D. Cal.), the first case filed against telecommunications service providers for allegedly assisting in the alleged warrantless surveillance program, and the lead case in the MDL-1791 proceeding. *See* Admin. Motion by Plaintiffs to Consider Whether Cases Should be Related (ECF No. 7) (Pls.' Mot. to Relate Cases); Plaintiffs' Motion for a Temporary Restraining Order at 2 (Pls.' Mot. for TRO) (ECF No. 186).

Jewel was brought by some of the same plaintiffs as in *Hepting*, but exclusively against the United States, its agencies, and current and former officials, whereas *Hepting* was against AT&T entities. Pls.' Motion to Relate Cases at 2-3. Notably, as Plaintiffs' motion to relate the cases expressly indicated: "both cases allege the same facts: that in 2001 the President authorized a program of domestic surveillance without court approval or other lawful authorization, and that through this Program, the government illegally obtains and continues to obtain with AT&T's assistance the contents of Plaintiffs' and class members' telephone and internet communications, as well as records concerning those communications." *Id*. at 3. *See also Jewel* Complaint at ¶ 7 ("In addition to eavesdropping on or reading specific communications, Defendants have indiscriminately intercepted the communications content and

[2] ECF numbers refer to filings in the *Jewel* case, unless otherwise indicated.

obtained the communications records of millions of ordinary Americans as part of the Program authorized by . . . President [Bush].").

In the fall of 2007, Plaintiffs in the MDL-1791 litigation, represented by the same counsel that represents the *Jewel* and the Plaintiffs in the *First Unitarian* case filed in 2013, moved the Court for an order requiring the preservation of evidence. Plaintiffs' Motion for Order to Preserve Evidence (ECF No. 373 in MDL-1791). Because the Government had asserted the state secrets privilege over facts necessary to litigate Plaintiffs' allegations of bulk collection of the content of the communications of millions of Americans and of bulk collection of communications records, the Government made clear in response to that motion that the parties were unable to discuss basic factual document preservation issues, such as what different types of potentially relevant information exists, where it is located, how it is being preserved, whether those steps are adequate, and whether additional steps are necessary or would be unduly costly or burdensome. *See* United States' Opposition to Plaintiffs' Motion for an Order to Preserve Evidence at 2 (ECF No. 386 in MDL-1791). Recognizing that it could not meaningfully confer with the Plaintiffs about basic document preservation issues, the Government submitted a classified declaration and supplemental memorandum with its opposition to the plaintiffs' motion that described how potentially discoverable information, if any, was being preserved. *See* United States' Notice of *In Camera, Ex Parte* Material (ECF No. 387 in MDL-1791). In its public opposition to the preservation motion, the Government referenced the classified record and offered to address any questions the Court might have about it in a classified setting. United States' Opposition to Plaintiffs' Motion for an Order to Preserve Evidence at 2 (ECF No. 386 in MDL-1791).

As the Court is aware, the Government has recently officially acknowledged the existence of certain NSA activities that were previously classified, and thus can now set forth on the public record some of the details of its classified submission and is filing herewith a declassified version of that submission. The purpose of the classified declaration submitted in response to the preservation motion in MDL-1791 was to "describe the policies and practices in place at NSA to preserve documents and information related to particular intelligence activities

authorized by the President after the 9/11 attacks that are implicated by the claims in this proceeding . . . ." Declassified Declaration of National Security Agency ¶ 2 (Declass. NSA Decl.) (attached hereto as Exh. A).[3]

The declaration made clear, in a number of places, that the plaintiffs challenged activities that occurred under presidential authorization, not under orders of the Foreign Intelligence Surveillance Court (FISC), and that the declaration was therefore limited to describing information collected pursuant to presidential authorization and the retention thereof. In particular, the declaration stated that "[b]ecause Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, this declaration does not address information collected pursuant to such an authorization or any retention policies associated therewith." Declass. NSA Decl. ¶ 12 n.4. The declaration also stated the following:

- "NSA is preserving a range of documents and communications concerning the presidentially-authorized activities at issue . . . ." *Id*. ¶ 6. The declaration described numerous categories of information being preserved, including Presidential authorizations, legal opinions and analysis, communications, content of communications intercepted under the TSP, intelligence reports containing TSP information, Internet and telephony metadata collected under the Presidential authorizations, reports of metadata analysis, briefing and oversight materials, and technical information. *Id*.

- The activities conducted pursuant to Presidential authorization—the interception of the content of communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization, the collection of Internet metadata, and the collection of telephony metadata—transitioned to FISC authorization. *Id*. ¶¶ 9-11.

- "I describe below the categories and preservation status of documents or information maintained by NSA [redacted] in the following three program activities prior to the relevant FISC Order for that activity: (i) The Terrorist Surveillance Program authorized by the President . . . (ii) The collection of non-content data concerning Internet communications authorized by the President ('Internet metadata')[;] (iii) The collection of telephone calling record information ('telephony metadata') authorized by the President." *Id*. ¶ 12.

- "As set forth below, the NSA [is] preserving documents and information potentially relevant to the claims and issues in this lawsuit with respect to the three categories of activities authorized by the President after 9/11 and detailed above for the period prior to the respective superseding FISC orders. NSA has taken various steps to ensure that staff and officials in offices that were cleared to possess information related to the presidentially authorized activities are preserving documents contained

[3] Again, this classified declaration specifically concerned preservation obligations in response to the allegations in *Hepting*, the predecessor case to which *Jewel* was related, and in *Shubert*, the sole remaining case before the Court from MDL-1791.

in their files and on their computer systems that relate to these activities. . . . [T]he General Counsel of the National Security Agency . . . instructed that information, records, or materials (including in electronic form) related to the presidentially-authorized activities be preserved." *Id.* ¶ 13.

- "To be clear, the presidentially authorized collection of internet metadata is segregated from information collected under the FISC Order of July 2004 and has not been destroyed." *Id.* ¶ 23.
- "The telephony metadata NSA collected [redacted] prior to the FISC order is segregated in an online database from that collected after May 2006 under the FISC Order . . . ." *Id.* ¶ 24.
- "For operational reasons, NSA maintains approximately five years worth of telephony metadata in its online database. Data acquired after 2003 under Presidential authorization is preserved electronically in an online data base. NSA has migrated to tapes telephony metadata collected during the period 2001-02, since the current operational relevance of that data has declined and continuing to maintain it on current operational systems would be unnecessary and would encumber current operations with more recent data." *Id.* ¶ 25.
- "NSA is preserving documentation of requests that it query its database of Internet and telephony metadata for analysis." *Id.* ¶ 26.
- "NSA is preserving documentation of its analysis of Internet and telephony metadata obtained pursuant to Presidential authorization and prior to the respective FISC Orders for these activities." *Id.* ¶ 27.
- "NSA is also preserving miscellaneous categories of administrative records related to the presidentially-authorized activities implicated by these lawsuits (TSP content collection, Internet metadata collection, telephony metadata collection)." *Id.* ¶ 28.

At the conclusion of the declaration, the Government offered to address any questions the Court may have had about the classified submission through secure *in camera, ex parte* proceedings. *Id.* ¶ 54.[4]

To address the preservation issues further in 2007, the Government submitted a classified memorandum in opposition to the Plaintiffs' motion for a preservation order as well. This memorandum also informed the Court that the NSA was preserving documents and information related to the presidentially-authorized activities, which may be relevant to the Plaintiffs' claims, not documents and information related to activities occurring pursuant to an order of the FISC, because the Plaintiffs' claims were that the challenged activities occurred without court approval. *See, e.g.*, Declassified Supplemental Memorandum of the United States in Opposition to

[4] The particular means by which the Government has preserved the information related to the presidentially-authorized activities may have changed since 2007, but that is irrelevant to the instant motion.

Plaintiffs' Motion for Order to Preserve Evidence at 3 n.4 (Declass. Mem.) (attached hereto as Exh. B) ("Because Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, the NSA classified submission does not address information collected pursuant to FISA authorization or any retention policies associated therewith."); at 8 ("As set forth by NSA, telephony metadata collected under presidential authorization is being preserved by NSA . . . ."); at 9 ("any discussion of the matter would also risk or require disclosure of the FISC Telephone Records Collection Order itself, to demonstrate an important limitation on the scope of potentially relevant evidence concerning telephony metadata."); at 10 ("NSA . . . preserves the [Internet] metadata collected prior to the July 2004 FISC Pen Register Order . . . .").

On November 6, 2007, the Court entered a preservation order in the MDL litigation (which, again, included *Hepting*, the predecessor to *Jewel*, and *Shubert*). ECF No. 393 in MDL-1791. In that order, the Court reminded the parties of their duties to preserve evidence that may be relevant to the claims in the action. *Id*. at 2. The Court instructed that preservation includes taking "reasonable" steps to prevent the destruction of information "reasonably anticipated to be subject to discovery . . . ." *Id*. at 3. Then the Court directed counsel "to inquire of their respective clients if the business practices of any party involve the routine destruction . . . of such materials and, if so, direct the party, *to the extent practicable for the pendency of this order*, either to (1) halt such business processes; (2) sequester or remove such material from the business process; or (3) arrange for the preservation of complete and accurate duplicates or copies of such material, suitable for later discovery if requested." *Id*. (emphasis added).

In November 2009, the parties in *Jewel* jointly moved the Court to enter a preservation order identical in substance to the MDL preservation order. ECF No. 50. On November 16, 2009, the Court issued the parties' proposed order, noting that it was based on the MDL order. ECF No. 51. The *Jewel* preservation order contains the language quoted above.

B. *First Unitarian* and the Government's Motion to the FISC for Permission To Preserve Telephony Metadata Collected under FISC Orders

Following the unauthorized disclosure in June 2013 of a FISC order, issued on April 25, 2013, which directed the production to the NSA of bulk call detail records, and the

Government's confirmation of the authenticity of that order, several plaintiffs filed suit in various United States District Courts challenging the legality of the Government's receipt of bulk telephony metadata pursuant to FISC orders.[5] The *First Unitarian* complaint, in contrast to the complaints in *Jewel*, *Shubert*, *Hepting*, and other cases in the MDL proceeding, challenge the legality of the Government's acquisition of bulk telephony metadata pursuant to FISC orders issued under Section 215 of the USA PATRIOT Act, Pub. L. No. 107-56 (2001) (Section 215), codified at 50 U.S.C. § 1861. For example, the *First Unitarian* complaint alleges that the NSA's alleged "Associational Tracking Program" "collects telephony communications information for all telephone calls transiting the networks of all major American telecommunication companies, including Verizon, AT&T, and Sprint, ostensibly under the authority of section 215 of the USA PATRIOT Act, codified at 50 U.S.C. § 1861." *First Unitarian* First Amended Complaint (FAC) ¶ 4. While the complaint alleges that the activity has been ongoing in various forms since October 2001, *id*. ¶ 8, it specifically discusses and attaches the April 25, 2013 FISC order purporting to authorize it, discusses Section 215, and specifically claims that the "Associational Tracking Program" "exceed[s] the conduct that may be lawfully authorized by an order issued under 50 U.S.C. § 1861." *Id*. ¶¶ 4, 52, 55-58, 66, 73, 103-108. Thus, *First Unitarian* puts the telephony metadata collected pursuant to the FISC's Section 215 orders directly at issue.

With respect to preservation of telephony metadata collected under FISA, the FISC's orders authorizing (and periodically reauthorizing) the NSA telephony metadata program, known as "Primary Orders," direct the NSA to strictly adhere to enumerated minimization procedures. These minimization procedures are required by Section 215 and ensure that the metadata are accessed for counter-terrorism purposes only. *See* 50 U.S.C. § 1861(g); *In re Application of the FBI for an Order Requiring the Production of Tangible Things, [etc.]*, Dkt. No. BR 13-80, Primary Order at 4-17 (F.I.S.C. Apr. 25, 2013) (ECF No. 66-5 in *First Unitarian*); Declaration of Teresa H. Shea (ECF No. 67-1 in *First Unitarian*) ("Shea *First Unitarian* Decl."), ¶¶ 30-35; March 7 FISC Op. & Order at 2. Among the minimization procedures in the Primary Order is a

[5] *See, e.g.*, *American Civil Liberties Union v. Clapper*, No. 13-cv-3994 (WHP) (S.D.N.Y.); *Klayman v. Obama*, Nos. 13-cv-851, 13-cv-881, 14-cv-092 (RJL) (D.D.C.); *Smith v. Obama*, No. 13-cv-00257 (D. Idaho); *First Unitarian Church v. NSA*, No. 3:13-cv-3287 (JSW) (N.D. Cal.); *Paul v. Obama*, No. 14-cv-0262 (RJL) (D.D.C.).

requirement that telephony metadata collected pursuant to FISC orders be destroyed no later than five years after their initial collection. Primary Order ¶ (3)E.

On February 25, 2014, the Government filed a motion with the FISC, on the public record, asking the FISC to amend its Primary Order to permit the retention of telephony metadata beyond five years after their initial collection, until relieved of its preservation obligation. The Government took this step to ensure compliance with any preservation obligations the Government may have in *First Unitarian* and other cases challenging the telephony metadata program authorized by FISC order. Exh. 1 to Govt. Defs.' Response to Pls' Mot. for TRO (ECF No. 188).[6] The Government specified that the metadata would be retained in a format that precludes any access or use by NSA intelligence analysts for any purpose, including to query the metadata for foreign intelligence purposes, and would be subject to further restrictions. *Id*. at 8.

On March 7, 2014, the FISC denied the Government's motion. Exh. 2 to Govt. Defs.' Response to Pls' Mot. for TRO. The FISC noted that under its orders authorizing the NSA's collection of telephony metadata under Section 215, the Government must comply with minimization requirements that include a requirement that call-detail records collected under the FISC's orders be destroyed within five years of their acquisition. *Id*. at 2. Although recognizing the general obligation of civil litigants to preserve records that could potentially serve as evidence in a case, the FISC observed that the statutory minimization requirements imposed by Section 215, 50 U.S.C. § 1861(g)(2), which the Primary Order implements, are intended to prevent the retention or dissemination of U.S. person information except as necessary to obtain, produce, or disseminate foreign intelligence information. *Id*. at 4. The FISC reasoned that the purpose for which the Government sought to retain the telephony metadata beyond five years—compliance with civil preservation obligations—was not related to obtaining, producing, or disseminating foreign intelligence information, and therefore that, at least on the record before it, could not find that an exception to Section 215's minimization requirements was permissible. *Id*. at 6-8. The FISC further noted that "no District Court or Circuit Court of Appeals has entered a

[6] Because, as explained above, *Jewel* and *Shubert* do not challenge the bulk collection of telephony metadata pursuant to FISA authorization, the Government did not mention those cases, or the preservation orders entered in them, in its motion to the FISC.

preservation order applicable to the [telephony] metadata in question in any of the civil matters cited in the motion" and that there was no indication that any of the plaintiffs had sought discovery of this information or made any effort to have it preserved, despite public knowledge of the Primary Order's destruction requirement. *Id*. at 8-9. The FISC also noted that destroying the metadata, not retaining it, was consistent with the substantive relief requested by the plaintiffs. *Id*. at 9. The FISC denied the motion "without prejudice to the government bringing another motion providing additional facts or legal analysis, or seeking a modified amendment to the existing minimization procedures." *Id*. at 12.

After receiving the FISC's order, the Government began to notify the plaintiffs in *First Unitarian*, and other cases challenging the FISC authorized telephony metadata program, of the FISC's March 7 order. Those notices stated that "[c]onsistent with that order, as of the morning of Tuesday, March 11, 2014, absent a contrary court order, the United States will commence complying with applicable FISC orders requiring the destruction of all call-detail records at this time." Gvt. Defs.' Notice Regarding Order of the FISC (ECF 85 in *First Unitarian*). On March 10, plaintiffs in *First Unitarian*, *Jewel*, and *Shubert* moved for a temporary restraining order preventing the Government from destroying the call-detail records, which the Court granted that same day, pending further briefing. ECF No. 189.

The next day, the Government notified the FISC of this Court's entry of a TRO and again moved the FISC for temporary relief from the telephony metadata destruction requirements pending resolution of the preservation issues raised by Plaintiffs in this Court. On March 12, the FISC issued an order granting the Government's motion for temporary relief from the five-year destruction rule, pending this Court's resolution of the preservation issues. Mar. 12, 2014 FISC Order (Exh. A to Pls.' Opening Brief re Evidence Preservation (ECF No. 191) (Pls.' Br.)). The FISC also ordered the Government to promptly notify the FISC of any additional material developments in civil litigation pertaining to the telephony metadata, including the resolution of the TRO proceedings in this Court. *Id*. at 7.

ARGUMENT

I. COMMON LAW PRESERVATION OBLIGATIONS IN CIVIL LITIGATION

When litigation is reasonably anticipated against a party, that party has a common law obligation to preserve—i.e., identify, locate, and maintain—information that is "relevant to specific, predictable, and identifiable litigation." *Apple Inc. v. Samsung Elec. Co., Ltd.*, 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012). "It is well-established that the duty pertains only to relevant documents." *Id.* (collecting cases). "Relevant" in this context means relevant for purposes of discovery, *see, e.g.*, Fed. R. Civ. P. 26(b)(1), 34(a)(1), including information that relates to the claims or defenses of any party, and that which is reasonably calculated to lead to the discovery of admissible evidence. *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18, 220 (S.D.N.Y. 2003) ("*Zubulake IV*").

Once the duty to preserve takes effect, the preserving party is "required to suspend any existing policies related to deleting or destroying files and preserve all relevant documents related to the litigation." *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006); *Apple Inc.*, 881 F. Supp. 2d at 1137; *see Jewel v. NSA*, 08-cv-04373, ECF No. 51 at 3 (ordering parties to halt destruction policies "to the extent practicable for the pendency of this order"). The common law duty to preserve relevant, discoverable information persists throughout the litigation. *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432-33 (S.D.N.Y. 2004) ("*Zubulake V*").

Reasonableness and proportionality are recurring touchstones informing the extent of a party's preservation obligation. *Apple Inc.*, 881 F. Supp. 2d at 1137 n.26, 1144; *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 523 (D. Md. 2010). *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 436 n.10 (S.D.N.Y. 2010). Because the duty to preserve "is neither absolute, nor intended to cripple organizations," *Victor Stanley, Inc.*, 269 F.R.D. at 523 (internal quotation omitted), courts have explained that preservation obligations require a litigant to take reasonable and proportional steps to preserve discoverable information under the circumstances. *Id.* at 522-23; *see also, e.g., Sloan Valve Co. v. Zurn Indus., Inc.*, 2012 WL

1886353, at *11-12 (N.D. Ill. May 23, 2012) ("A party fulfills its duty to preserve evidence if it acts reasonably."). Determining whether preservation conduct is acceptable in a given case "depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case." *Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010); *see also Pippins v. KPMG LLP*, 279 F.R.D. 245, 255 (S.D.N.Y. 2012) (explaining that this inquiry "depends heavily on the facts and circumstances of each case and cannot be reduced to a generalized checklist of what is acceptable or unacceptable") (internal quotations omitted).

Because "[p]reservation and production are necessarily interrelated," application of the proportionality and reasonableness principles to preservation "flow[] from the existence of th[ose] principle[s] under the Federal Rules of Civil Procedure." *Pippins*, 279 F.R.D. at 255 ("[P]roportionality is necessarily a factor in determining a party's preservation obligations."); *Orbit One Commc'ns, Inc.*, 271 F.R.D. at 436 n.10 ("Reasonableness and proportionality are surely good guiding principles for a court that is considering imposing a preservation order.").

To that end, Rule 26(b)(2)(C)(iii)'s "'proportionality' test for discovery" applies to the preservation context, *Pippins*, 279 F.R.D. at 255, insofar as it requires courts to "limit the frequency or extent of discovery," and thus the scope of preservation, where its "burden or expense . . . outweighs its likely benefit considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues." Fed. R. Civ. P. 26(b)(2)(C)(iii); U.S. District Court for the Northern District of California, Guidelines for the Discovery of Electronically Stored Information (ESI), Guideline 1.03 ("The proportionality standard set forth in Fed. R. Civ. P. 26(b)(2)(C) . . . should be applied to," *inter alia*, "the preservation . . . of [electronically stored information (ESI)]."); *see also Pippins*, 279 F.R.D. at 255 (citing *The Sedona Conference Commentary on Proportionality in Electronic Discovery*, 11 Sedona Conf. J. 289, 291 (2010) ("The burdens and costs of preservation of potentially relevant information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation. . . . Technologies to reduce cost and burden

should be considered in the proportionality analysis.")).[7] For this reason, courts considering a party's preservation obligations, including whether additional preservation measures are necessary, balance the burden of preserving certain information with the moving party's showing of its relevance. *See, e.g., Young v. Facebook, Inc.*, 2010 WL 3564847, at *1 (N.D. Cal. Sept. 13, 2010); *Jardin v. Datallegro, Inc.*, 2008 WL 4104473, at *1 (S.D. Cal. Sept. 3, 2008); *Columbia Pictures Indus. v. Bunnell*, 2007 WL 2080419, at *4-6, 13 (C.D. Cal. May 29, 2007); *Donini Intern., SPA v. Satec, LLC*, 2006 WL 695546, at *8 (S.D.N.Y. Mar. 16, 2006).

In applying these principles here, it is important for the Court to bear in mind exactly what information is at issue. The FISC's orders governing the telephony metadata program allow the NSA to keep up to five years' worth of data; the dispute here concerns only data that the NSA would otherwise destroy to comply with that five-year retention limit. Thus, the question is whether the benefit to Plaintiffs' case of preserving data the NSA would otherwise age-off to comply with the FISC's five-year limit outweighs the burdens of preserving those data—and countervailing public policy—when the NSA would continue in all events to retain a much larger body of metadata for operational purposes. Plaintiffs barely address, however, the issue they themselves have raised. Instead, they devote the lion's share of their arguments to the proposition that the *Jewel* preservation order already requires preservation of data collected by the NSA under FISC authorization. As discussed below, that argument has no merit.

II. THE GOVERNMENT HAS COMPLIED FULLY AND IN GOOD FAITH WITH THE PRESERVATION ORDERS ISSUED IN *JEWEL* AND *IN RE NSA TELECOMMUNICATIONS RECORDS LITIGATION*, WHICH DO NOT REQUIRE PRESERVATION OF DATA ACQUIRED UNDER FISC AUTHORITY

Consistent with its preservation obligations and the preservation orders entered in *Jewel* and *In re NSA Telecommunications Records Litigation* (MDL-1791) (which includes *Shubert*), the Government has preserved a wide swath of documents and information related to particular NSA intelligence activities authorized by President Bush after 9/11 (*i.e.*, the Terrorist

[7] *See also, e.g.*, Fed. R. Civ. P. 26(b)(2)(B) (establishing additional limitations on the discovery of ESI, including ESI "not reasonably accessible because of undue burden or cost"); *id.* Advisory Comm. Notes to 2006 Amendments (stating that such burdens and costs are properly considered as part of the proportionality analysis).

Surveillance Program, and the Internet and telephony metadata programs). Prior to the entry of those orders, however, the Government had expressly advised the Court that it did not consider those obligations and orders to extend to information collected pursuant to FISC orders, including the FISC's telephony metadata orders, because the Plaintiffs in *Jewel* and *In re NSA Telecommunication Records Litigation* challenged activities occurring without a court order. The Government's position on the matter, which is supported by the complaints themselves, was set forth in a detailed classified submission lodged with the Court prior to the entry of the preservation order in the MDL-1791 proceeding—the order upon which the subsequent *Jewel* preservation order was based. Moreover, the Government has maintained this understanding about the scope of the complaints in *Jewel* and *In re NSA Telecommunication Records Litigation* throughout the litigation and has not represented otherwise, as plaintiffs now erroneously contend.

In litigating the MDL plaintiffs' motion for an order to preserve evidence, the Government informed the Court in October 2007 in a classified filing about the documents and information it was preserving. Numerous categories of documents and information were being preserved related to the President's Surveillance Program (which at the time was still classified except for the existence of the TSP), including Presidential authorizations, legal opinions and analysis, communications, content of communications intercepted under the TSP, intelligence reports containing TSP information, Internet and telephony metadata collected under the Presidential authorizations, reports of metadata analysis, briefing and oversight materials, and technical information. Declass. NSA Decl. at ¶ 6; Declass. Mem. at 4-5. As clearly stated in that declaration and brief, the NSA was preserving, pursuant to its litigation preservation obligations, a range of documents and information concerning the presidentially-authorized activities at issue in the plaintiffs' complaints, but not information about activities conducted pursuant to FISC orders. The Government specifically explained that "[b]ecause Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, this declaration does not address information collected pursuant to such an authorization or any retention policies associated therewith." Declass. NSA Decl. ¶ 12 n.4; *see also* Declass. Mem. at 3 n.4.

Rather, the purpose of the declaration was "to describe the policies and practices in place at NSA to preserve documents and information related to particular intelligence activities authorized by the President after the 9/11 attacks that are implicated by the claims in this proceeding . . . ." Declass. NSA Decl. ¶ 2. The submission specifically addressed telephony and Internet metadata, explaining that metadata collected under presidential authorization had been segregated from that collected under FISC order, and that NSA was preserving the metadata collected under presidential authorization prior to the entry of the FISC orders. Declass. NSA Decl. ¶¶ 23-24; Declass. Mem. at 4, 8, 10. *See also, e.g.*, Declass. NSA Decl. ¶ 6 (NSA is preserving "Internet and telephony metadata collected under the Presidential authorization"). The Government further described the FISC telephony metadata and Internet metadata orders as "important limitation[s] on the scope of potentially relevant evidence . . . ." Declass. Mem. at 9, 11.[8]

Following this submission, the Court entered a preservation order that contained language consistent with the Government's classified submission. The parties were instructed to preserve evidence "that may be relevant to this action" and that there was a reasonableness limitation to preservation. Nov. 6, 2007 Preservation Order (ECF No. 393) at 3 (preservation includes taking "reasonable" steps to prevent the destruction of information "reasonably anticipated to be subject to discovery . . . ."). The Court directed counsel "to inquire of their respective clients if the business practices of any party involve the routine destruction . . . of such materials and, if so, direct the party, *to the extent practicable for the pendency of this order*, either to (1) halt such business processes; (2) sequester or remove such material from the business process; or (3)

[8] Although the existence of these activities has now been declassified, they were highly classified at the time the parties were litigating the preservation order in the MDL litigation and at the time the *Jewel* preservation order was entered, and have been until very recently. Thus, Plaintiffs' suggestion that had the Government had any question about the scope of its preservation obligations and what specific documents it was supposed to preserve (which it did not, in light of the nature of the allegations in *Jewel*), it could have simply "pick[ed] up the phone and call[ed] opposing counsel," Pls.' Br. at 10, is patently specious and ignores the fact that the highly classified nature of the documents and information at issue foreclosed any consultation on these matters, as the Government repeatedly made clear in response to the preservation motion itself. The Government fulfilled its duties, including by informing the Court in a classified filing of the evidence it was preserving, and it offered to answer any questions that the Court may have had, in a classified setting.

arrange for the preservation of complete and accurate duplicates or copies of such material, suitable for later discovery if requested." *Id.* (emphasis added). It would not have been practicable for the Government to preserve data beyond five years in violation of FISC orders.[9]

The complaints, both in the MDL-1791 litigation in which the preservation order was first issued (which included the *Jewel* plaintiffs' prior lawsuit in *Hepting* and *Shubert*), and in *Jewel* fully support the Government's approach to preservation in these cases. The lynchpin of the MDL cases, including *Hepting* and *Shubert*, was the claim that the alleged government program to intercept telephone, Internet, and email communications and communications records was done without the authorization of any court, including the FISA court.[10]

Indeed, the MDL-1791 litigation, which was predominantly brought against telecommunications service providers, had to, as a practical matter, claim that the challenged activity occurred without a court order, because several federal statutes protect private parties

---

[9] It bears noting that the court hearing the preservation matter did not question the Government's approach to preservation or instruct the Government to preserve information related to the FISC-authorized programs, which had been described by the Government to the court repeatedly in classified declarations in support of the state secrets privilege dating back to 2006.

[10] *See, e.g.*, *Hepting* Amended Complaint (Am. Cmplt.) at ¶ 2 ("This case challenges the legality of Defendants' participation in a secret and illegal government program to intercept and analyze vast quantities of Americans' telephone and Internet communications, surveillance done without the authorization of a court and in violation of federal electronic surveillance and telecommunications statutes, as well as the First and Fourth Amendments to the United States Constitution."), ¶ 3 ("This surveillance program, purportedly authorized by the President at least as early as 2001 and primarily undertaken by the National Security Agency ("NSA") without judicial review or approval, intercepts and analyzes the communications of millions of Americans."); *Shubert* Second Amended Complaint (SAC), filed May 8, 2012, ¶ 2 ("Without the approval of Congress, without the approval of any court, and without notice to the American people, President George W. Bush authorized a secret program to spy upon millions of innocent Americans, including the named plaintiffs."), ¶ 9 ("This class action is brought on behalf of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, a court order, or other lawful authorization since September 12, 2001."), ¶ 55 ("Although it is true that federal law requires law enforcement officers to get permission from a federal judge to wiretap, track, or search, President Bush secretly authorized a Spying Program that did none of those things."), at ¶ 66 ("The Program admittedly operates 'in lieu of' court orders or other judicial authorization . . . ."), ¶ 93 ("Prior to its initiation, defendants never sought authorization from the FISA Court to conduct the Spying Program."); Master Consolidated Complaint Against MCI Defs. and Verizon Defs. (ECF No. 125 in MDL-1791) ¶ 3 ("This case challenges the legality of Defendants' participation in an illegal federal government program to intercept and analyze vast quantities of Americans' telephone and electronic communications and records, surveillance done without any statutorily authorized permission, customers' knowledge or consent, or the authorization of a court . . . .").

from suit for providing assistance to the Government at the direction of a court order. *See* 50 U.S.C. § 1861(e) (FISA); 18 U.S.C. §§ 2707(e), 2703(e) (ECPA); 18 U.S.C. § 2511(2)(a)(ii) (Wiretap Act). Moreover, the factual allegations of the complaints are the facts about the presidentially-authorized activities—*i.e.*, the collection of communications content and records under the President's Surveillance Program. *See Shubert* SAC ¶¶ 53-96; Master Consol. Cmplt. at ¶¶ 136-158; *Hepting* Am. Cmplt. ¶¶ 32-41.

Although the Plaintiffs in *Jewel* sued the Government, not telecommunications service providers, their complaint too is unmistakably about the presidentially-authorized intelligence activities allegedly conducted without a court order. *See, e.g.*, *Jewel* Complaint at ¶ 7 ("In addition to eavesdropping on or reading specific communications, Defendants have indiscriminately intercepted the communications content and obtained the communications records of millions of ordinary Americans as part of the Program authorized by . . . President [Bush]."), ¶ 39 (President Bush "authoriz[ed] "a range of surveillance activities . . . without statutory authorization or court approval, including electronic surveillance of Americans' telephone and Internet communications (the 'Program')"), ¶ 76 ("Defendants' above-described acquisition in cooperation with AT&T of . . . communications content and non-content information is done without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority."), ¶ 92 ("Defendants' above-described solicitation of the disclosure by AT&T of . . . communications records . . . is done without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority."), ¶¶ 110, 120, 129, 138 ("Defendants have [acquired] . . . contents of communications, and records pertaining to . . . communications . . . without judicial, statutory, or other lawful authorization, in violation of statutory and constitutional limitations, and in excess of statutory and constitutional authority.").

Moreover, the *Jewel* Plaintiffs did not make any effort to amend their Complaint and challenge collection of communications content under FISA orders, despite the public announcement in January 2007 that the TSP had transitioned to FISA orders. *See* Pls.' Rule

1006 Summary of Evidence (ECF No. 30-1) at 46. Nor did Plaintiffs seek to challenge content collection under Section 702 of the FISA, 50 U.S.C. § 1881a, or its precursor, the Protect America Act of 2007 (PAA), despite the fact that both of those statutes preceded the filing of the *Jewel* Complaint (and Section 702 had even been challenged in federal district court, *see Clapper v. Amnesty International*, 133 S. Ct. 1138, 1146 (2013)). In fact, the *Jewel* Plaintiffs stated in their summary of evidence filed on June 3, 2009 that "none of the assistance alleged in the various complaints was provided pursuant to the PAA." ECF No. 30-1 at 49. Thus, despite public acknowledgement that the content collection aspect of "the Program" authorized by the President after the 9/11 attacks was now subject to FISC orders and, later, statutory authority—which began over *one year before* the *Jewel* Complaint was filed in September 2008—the *Jewel* plaintiffs did nothing to change their allegations in *Hepting* or proceed to challenge any FISA authorized activities in the *Jewel* Complaint. Plaintiffs thereafter continued to frame their claims as challenges to the legality of the presidentially-authorized activities in subsequent briefing. For example, in the most recent round of dispositive briefing in 2012, Plaintiffs in *Jewel* and *Shubert* discussed the facts of the President's Surveillance Program, not the FISC orders pursuant to which the activities had transitioned. *See, e.g.*, Plaintiffs' Motion for Partial Summary Judgment at 6-9 (ECF no. 83); Plaintiffs' Opposition to Defs.' Third Motion to Dismiss and for Summary Judgment (ECF No. 76 in *Shubert*) at 2-5, 18.

Accordingly, Plaintiffs' effort to recast the *Jewel* Complaint as challenging FISC-authorized activities is nothing more than a post-hoc, unfounded attempt to rewrite their Complaint in order to create a preservation dispute in *Jewel* concerning previously classified matters. All of Plaintiffs' specific contentions in support of this theory are meritless. Plaintiffs first point to the statement in their Rule 56(f) declaration that they intended to take discovery regarding the fact of carriers' interception and disclosure of the communications and communications records of customers (Pls.' Br. at 7). But that indicates nothing more than that they seek discovery concerning an allegation in the complaint that records were collected pursuant to presidential authorization in "the Program," and does not remotely indicate Plaintiffs

are challenging a FISC-authorized collection or records, nor does it undermine the Government's understanding of Plaintiffs' claims.

Plaintiffs also point to references to now declassified FISC activities wholly out of context in an effort to show their Complaint must challenge activities undertaken *with* judicial authority. Plaintiffs cite references they made to "post-FISC transition surveillance" in the Joint Case Management Statement filed by the parties on September 20, 2013 (ECF No. 159). Pls.' Br. at 7. But those references concern what Plaintiffs claim to be the Government's official disclosures following the unauthorized disclosures that began in June 2013—the subject the joint statement was supposed to address—and which prompted the Court to require further briefing on the national security issues in this case. *See* Jt. Statement at 4-5. Nothing Plaintiffs said in the joint statement indicated they were now challenging FISC-authorized activities. Plaintiffs further argue that in the Government's section of the joint statement, "rather than asserting its current, cramped claims about the scope of the *Jewel* claims, the government instead conceded that 'Plaintiffs claim this alleged 'dragnet' surveillance included collection of the content of telephone and Internet communications as well as communications records." Pls.' Br. at 7-8. Again, this wrenches a snippet of text out of context. In the immediately preceding sentence, the Government specifically referred to the activities authorized by President Bush. Jt. Statement at 33 ("In the above-captioned *Jewel* and *Shubert* cases, Plaintiffs allege that, following the 9/11 terrorist attacks, then-President George W. Bush authorized the National Security Agency (NSA) to undertake, with the assistance of major telecommunications companies, indiscriminate warrantless surveillance of the communications of millions of Americans."). Nothing stated by the Government remotely concedes that the *Jewel* Complaint challenges judicially-authorized FISC activities.

Nor did the Government concede that Plaintiffs' claims included the FISC-authorized activities in the now-declassified declarations submitted in the *Jewel* and *Shubert* cases. Pls.' Br. at 8-9. Plaintiffs badly misconstrue these declarations in making this argument. Those declarations, submitted in support of the Government's state secrets privilege assertion prior to the recent disclosures, simply provided the Court with a then-classified fact: that the

presidentially authorized activities that were being challenged in *Jewel* had been subsequently transitioned to FISC-authorized activities. The Government's then-classified declarations consistently described Plaintiffs' claims as being about the presidentially-authorized activities only. *See, e.g.*, 2009 DNI Decl. ¶ 3 ("In sum, plaintiffs allege that, after the 9/11 attacks, the NSA received presidential authorization to engage in surveillance activities far broader than the publicly acknowledged 'Terrorist Surveillance Program' ('TSP') . . . Plaintiffs allege that the NSA, with the assistance of telecommunications companies including AT&T, has indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans as part of an alleged presidentially-authorized 'Program' after 9/11."); 2013 NSA Unclass. Decl. ¶ 18 ("In sum, plaintiffs allege that, after the 9/11 attacks, the NSA received presidential authorization to engage in 'dragnet' communications surveillance in concert with major telecommunications companies. . . . Plaintiffs allege that, pursuant to presidential authorization and with the assistance of telecommunications companies (including AT&T and Verizon), the NSA indiscriminately intercepted the content and obtained the communications records of millions of ordinary Americans.").[11]

Thus, to the extent the classified declarations discussed the fact that the presidentially-authorized activities transitioned to orders of the FISC, they did so to show that disclosing or confirming these activities under Presidential authorization in order to litigate Plaintiffs' claims would risk the disclosure of ongoing, highly classified intelligence operations authorized by the FISC, causing exceptional harm to national security. For instance, the NSA's declarant explained in 2012 as follows:

> While the plaintiffs' allegations are focused on the period immediately following 9/11, and seek to challenge alleged activities undertaken pursuant to presidential authorization, the sources and methods used by NSA at that time continue to be used under subsequent authorizations. To expose a source and method, based on its use during one period of time, under one authority, would

[11] *See also* United States' Reply in Support of Mot. to Dismiss or, in the Alternative, for Summ. Judgment (ECF No. 520 in MDL-1791) at 32 n.29 ("All of the claims in this litigation are premised on the alleged absence of court orders in support of the alleged activities . . . ."). Plaintiffs' quotation from the Plaintiff-Appellees' Ninth Circuit Reply Brief in the 2010 *Jewel* appeal confirms that the Government has not hid its understanding of the *Jewel* Complaint as not challenging surveillance authorized by the FISC. Pls.' Br. at 9-10.

> compromise, if not destroy, NSA's ability to use that method today. All of the presidentially authorized activities being challenged in this lawsuit (starting in July 2004) were placed under other FISA authority and have been subject to Congressional oversight. The need to protect these sources and methods continues to exist notwithstanding plaintiffs' challenge to the lawfulness of their use under presidential authorization.

2012 NSA Decl. ¶ 52. *See also id*. ¶¶ 7, 34, 37, 84; 2007 DNI Decl. ¶ 3; 2007 NSA Decl. 62-64; 2009 DNI Decl. ¶ 40-41; 2009 NSA Decl. ¶¶ 26-27, 57- 67; 2012 DNI Decl. ¶ 56-57.

In sum, the claims in *Jewel* and *In re NSA Telecommunications Records Litigation*, including *Shubert*, were clearly directed at presidentially-authorized NSA intelligence activities, unauthorized by a court order, and the Government correctly construed its preservation obligations as limited to such activities. Nonetheless, rather than remaining silent on its assessment of what information should be preserved, the Government, at the time of the first preservation motion, specifically informed the Court in a detailed, classified filing of precisely how it was satisfying its preservation obligations, and in particular the fact that it was only preserving those materials related to the presidentially authorized activities, not to FISC authorized activities, consistent with Plaintiffs' claims. In these circumstances, where the complaint challenges alleged surveillance activities undertaken without judicial authorization and in violation of statutory requirements, including under the FISA, and where the Government expressly advised the Court of its preservation steps before the entry of the preservation order, Plaintiffs' contention that the preservation obligations in *Jewel* extended to preserving data that were collected pursuant to judicial order, subject to statutory requirements set forth in the FISA (including requirements to minimize the retention of such records), is entirely without merit.

Indeed, Plaintiffs' position fails entirely to appreciate the circumstances facing the Government after the FISC orders were implemented. Despite the fact that Plaintiffs had challenged alleged presidentially-authorized activities undertaken *without* judicial orders and *outside of* FISA limitations, the Government knew at the time the 2007 preservation order was being litigated that two of those activities (Internet and telephony metadata collection) had already transitioned to FISC-approved classified programs, and so advised the Court in a classified filing. And by the time the *Jewel* Complaint had been filed in September 2008, the

third presidentially-authorized activity (the collection of content) had also publicly transitioned to FISA without any challenge from Plaintiffs. The transition of these activities to FISC authorization was intended to address the core concern that presidentially-authorized surveillance programs be placed under judicial supervision and subjected to statutory requirements—the very concern raised in the MDL-1791 litigation and again in *Jewel*. Plaintiffs nevertheless take the position that the Government could only have met its preservation obligations in *Jewel* if it indefinitely suspended the restrictions on the retention of data imposed by the FISC—the Article III court vested by Congress with jurisdiction to issue orders authorizing foreign intelligence surveillance activities and enforcing statutory restrictions on the retention of data under the FISA—just as they were being put in place, on the assumption that the *Jewel* Plaintiffs might later claim that the FISC lacked authority to implement those activities. Plaintiffs' position is nothing more than post-hoc second-guessing of the preservation efforts undertaken in connection with *Jewel* and *Shubert*, entirely unsupported by their own complaints and the record of this case when preservation orders were litigated.

III. WHETHER THE COURT SHOULD ORDER PRESERVATION OF METADATA COLLECTED UNDER FISC-AUTHORIZATION FOR PURPOSES OF *FIRST UNITARIAN* REQUIRES THE COURT TO BALANCE THE BURDENS OF PRESERVATION ON THE GOVERNMENT AGAINST PLAINTIFFS' SHOWING OF THE DATA'S VALUE TO THEIR CASE.

Leaving aside Plaintiffs' meritless contention that the preservation order in *Jewel* should now be read, in *post-hoc* fashion, to apply to FISC-authorized activities, the question remains how preservation obligations should apply going forward in the *First Unitarian* litigation, a lawsuit that expressly challenges the collection of telephony metadata under FISC authorization pursuant to Section 215. Even as to FISC-authorized collection of telephony metadata for *First Unitarian*, the court must balance any benefit of Plaintiffs' (hypothetical) access to metadata that the NSA would otherwise age off against the costs and burdens placed on the NSA of preserving the data. The Government addresses below two possible options for preserving telephony metadata that the NSA would otherwise age off to comply with the FISC's five-year retention limit: (1) targeted preservation only of data pertaining to Plaintiffs' calls (assuming, without confirming or denying, that the NSA has in fact collected metadata pertaining to Plaintiffs'

calls); or (2) mass preservation of all telephony metadata pertaining to calls to, from, or within the United States that would otherwise be aged off. Both options involve significant obstacles and burdens, and the latter would contravene important public policies underlying FISA.

A. Targeted Preservation of Data Pertaining Only to Plaintiffs' Calls (if Any) Would Be Burdensome and Impractical.

Although Plaintiffs have not expressly requested it, one theoretical option for preserving metadata the NSA would otherwise age off would be targeted preservation of any metadata that pertain only to Plaintiffs' calls. Of course, the Government cannot confirm or deny whether it has, in fact, collected metadata pertaining to any of the Plaintiffs' calls, but in either event the attempt to ascertain whether the NSA has collected data regarding Plaintiffs' calls, and then to preserve only those data, would be burdensome and impractical.

Before beginning to preserve any telephony metadata associated only with Plaintiffs' calls, the NSA would first have to determine whether it had collected any such data in the first instance. Given that the telephony metadata the NSA collects does not include the identity of the subscriber of the party making or receiving the call, *see* Shea Public Decl. ¶ 3 n.1, each Plaintiff organization and each individual Plaintiff would have to provide the NSA with all telephone numbers that each had used or been assigned at any time since 2009, as well as the time periods during which each Plaintiff was assigned or used a particular number. *See id.* ¶ 11. Indeed, as this litigation continues, each Plaintiff would need to keep the Government apprised of any changes in the telephone numbers used by, or assigned to, that Plaintiff. *See id.*

In the event each Plaintiff agrees to turn over that information (and update it as necessary) for use by the NSA in complying with a targeted preservation order, the NSA would need to run queries of its database using these telephone numbers as terms to determine whether the NSA has collected and retained data associated with Plaintiffs' calls. *See id.* ¶ 13. Prior to doing so, however, the Government may have to seek and obtain approval from the FISC, because FISC orders permit the NSA only to run queries of the database for foreign intelligence purposes, using identifiers (e.g., telephone numbers) that are reasonably suspected of being associated with foreign terrorist organizations that have been approved for targeting by the FISC.

See id.; *see also, e.g.*, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]* (Oct. 11, 2013) ("Oct. 11, 2013 FISC Op. and Order") at 6.[12]

Presuming that the FISC were to grant approval to the NSA to conduct these otherwise prohibited queries, and presuming further that metadata associated with Plaintiffs' calls have been collected and retained by the NSA, queries using Plaintiffs' telephone numbers would return records of their calls including (among other data) the telephone numbers of the persons and organizations with which each Plaintiff was in contact over a period of time that would vary depending on how long the NSA would be required to preserve data that it would otherwise destroy. *See* Shea Public Decl. ¶ 13. Once the metadata pertaining only to Plaintiffs' calls (if any) were extracted and isolated, the Government would then need to seek and obtain FISC approval to retain any data on an ongoing basis that otherwise should be aged off in compliance with all of the FISC orders requiring destruction of metadata "no later than five years (60 months) after its initial collection." *E.g.*, Oct. 11, 2013 FISC Op. and Order at 14.[13] Presuming that the FISC approved the targeted preservation of the telephony metadata associated with Plaintiffs' calls for the duration of this litigation, the NSA would have to separately maintain this collection of records about Plaintiffs' calls in order to ensure that only these metadata, and not metadata pertaining to calls that were not made to or from Plaintiffs' numbers, would be preserved beyond the five-year period permitted under the governing FISC orders. *See* Shea Public Decl. ¶ 13.

This type of targeted preservation appears inconsistent, however, with the privacy concerns Plaintiffs have repeatedly expressed in this litigation. In one of their earlier submissions to the Court, Plaintiffs in *First Unitarian*, for example, expressed concern that the telephony metadata program "provides the NSA with the capability to build a deeply invasive

[12] The leave the FISC has temporarily granted the NSA to access the metadata for civil litigation purposes expires upon "resolution of the preservation issues" presented here. March 12 FISC Op. & Order at 6-7.

[13] The Government would need to seek such approval, notwithstanding the FISC's recent order granting the Government relief from this destruction obligation, because that order also constituted only "temporary relief from the five-year destruction requirement" until "resolution of the preservation issues" in the above-captioned actions. *See* March 12 FISC Op. & Order at 6.

associational dossier of each of [them] through tracking their communications." Pls.' Reply and Opp. (ECF No. 72 in *First Unitarian*) at 37. These Plaintiffs also claim in their declarations that third-parties with whom they communicate—the very communications they seek to keep private but whose communications with Plaintiffs would be isolated and preserved by any targeted preservation order—echo Plaintiffs' concerns about their calls being monitored, logged, or otherwise tracked by the NSA. *See, e.g.*, Acorn Decl. ¶ 8; Students for Sensible Drug Policy Decl. ¶ 6; Bill of Rights Comm. Decl. ¶ 8b; Franklin Armory Decl. ¶ 4; Unitarian Universalist Decl. ¶ 4; Free Software Decl. ¶¶ 4c, 5; Free Press Decl. ¶¶ 4, 5; CAL-FFL Decl. ¶ 4; Media Alliance Decl. ¶ 6; First Unitarian Decl. ¶¶ 4c, 8; CAIR-F Decl. ¶ 4d; CAIR-CA Decl. ¶ 11; s*ee also* First Am. Compl. ¶ 77.

Targeted preservation would also impose significant burdens on the NSA, as detailed in the Classified NSA Declaration submitted *ex parte*, *in camera*, concurrent with this filing. Assuming that the NSA has collected and retained metadata associated with Plaintiffs' telephone calls, the NSA would have to devote significant financial and personnel resources over several months—assets that otherwise would be devoted to the NSA's national security mission—to create, test, and implement a solution (or series of solutions) that would accomplish the preservation of only the targeted metadata on an ongoing basis for the duration of this litigation. *See* Shea Public Decl. ¶ 14. The fact that the NSA does not know how long this litigation will continue, coupled with ever-changing mission requirements and systems, make it extremely difficult to estimate specific costs and to devise the most effective solution should this Court issue an order requiring preservation of data that otherwise would be subject to age-off pursuant to longstanding requirements of the FISC. Nevertheless, to the extent possible at this stage, the NSA has detailed how it would identify, extract, and preserve any records associated with Plaintiffs' calls as that data is ready to age-off its system in the classified, *ex parte* NSA declaration submitted herewith. Similarly, details regarding the nature and extent of the burden a targeted preservation order would impose on the NSA cannot be addressed in this filing and are covered in the same classified, *ex parte* declaration.

B. Mass Preservation of Bulk Telephony Metadata that the NSA Otherwise Would Age Off Would Also Impose Significant Burdens on the NSA and Contravene Public Policy Underlying FISA's Minimization Requirements.

An alternative to the targeted preservation of metadata (if any) pertaining only to Plaintiffs' telephone calls would be the mass preservation for purposes of *First Unitarian* of all telephony metadata that the NSA would otherwise age off in compliance with the five-year limit on retention of the data imposed by the FISC's orders. This approach could also require the diversion of significant financial, technological, and personnel resources from the pursuit of NSA's core national security mission, and would disserve important public policies that underlie FISA's statutory scheme.

As described in the classified NSA declaration that the Government is submitting herewith for *ex parte* review, the amount of data involved is voluminous, and would grow over time depending on the duration of the litigation in these cases. Maintaining the data and thereafter making them accessible for (hypothetical) discovery purposes[14] would impose significant burdens on the financial, technological, and personnel resources of the NSA, that are detailed in the classified NSA declaration. In unclassified terms, the NSA has essentially two options for mass retention of the data. Both could involve significant software development costs to create the capability to transfer data from the operational database to the preservation medium as they age off. The first option would thereafter place considerable burdens on the NSA's information technology and personnel resources that would remain ongoing, and in fact increase, as time passes. The second option would be more cost-effective, and less burdensome so far as preservation of the data are concerned. Assuming hypothetically, however, that the data would have to be produced for purposes of litigation, the second option would require significant investments of time—up to several months—by NSA personnel, and a corresponding investment of NSA technological resources, to make the data accessible, all of which would have to be diverted from pursuit of NSA's core mission to collect, process, and disseminate signals intelligence for purposes of national security. *See generally* Classified NSA Declaration.

[14] As noted below, the data at issue here are classified and are subject to the assertion of the state secrets privilege by the Director of National Intelligence (DNI) in *Jewel.*

The singular circumstances of this litigation also present an additional public policy consideration that the Court should take into account when determining whether mass preservation of the telephony metadata that the NSA would otherwise age off to comply with the FISC's orders is justified by Plaintiffs' need. As noted above, and as the Government has explained in *First Unitarian*, the FISC's orders authorizing the NSA's collection of bulk telephony metadata under Section 215 require that the "metadata shall be destroyed no later than five years (60 months) after [their] initial collection." *See, e.g.*, *In re Application of the FBI for an Order Requiring the Production of Tangible Things, [etc.]*, Dkt. No. BR 13-80, Primary Order at 14 (F.I.S.C. Apr. 25, 2013) (ECF No. 66-5 in *First Unitarian*) ("Primary Order"); *see also* Declaration of Teresa H. Shea (ECF No. 66-1 in *First Unitarian*) ("Shea *First Unitarian* Decl."), ¶ 30; March 7 FISC Op. & Order at 2. This destruction requirement is the crux of the instant dispute between the Plaintiffs and the Government, but it involves more than a conflict between the obligation of a litigant to preserve potentially relevant evidence and the Government's duty to comply with the orders of an Article III court such as the FISC.

As the Government explained in support of its motion to dismiss the complaint in *First Unitarian*, the FISC's orders authorizing the NSA's bulk collection of telephony metadata under section 215 of the USA-PATRIOT Act, Pub. L. No. 17-56, 115 Stat. 272 (2001) ("Section 215"), codified at 50 U.S.C. § 1861, also require the Government to comply with "minimization procedures" that strictly limit access to and review of the metadata, and limit dissemination of information derived therefrom, to valid counter-terrorism purposes. *See* Gov't Defs.' Mot. to Dismiss & Opp. to Pls' Mot. for Partial Summ. Judg. (ECF No. 66 in *First Unitarian*) at 6-8; Primary Order at 4-17. The FISC's imposition of such minimization procedures is required by the terms of Section 215 itself, which provides that an order directing the production of documents, records, or other tangible items under authority of the statute "shall direct" that the Government also follow specific "minimization procedures," adopted by the Attorney General,

> that are reasonably designed … to minimize the *retention*, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1861(c)(1), (g(2)(A) (emphasis added). The five-year limit on retention of telephony metadata after their collection is one of the minimization procedures that the FISC has consistently imposed on the NSA as a condition on its authorization of the telephony metadata program. *See* Shea *First Unitarian* Decl. ¶ 30; Primary Order at 14.

The imposition of detailed minimization procedures limiting the retention and dissemination of information pertaining to U.S. persons for purposes other than foreign intelligence is not peculiar to Section 215. Minimization procedures are an essential feature of FISA's statutory scheme. The Government's adoption and the FISC's approval and enforcement of specific minimization procedures "that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination" of information concerning U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information," 50 U.S.C. § 1801(h)(1), are also statutory pre-requisites to the authorization of electronic surveillance under Title I of FISA, *id.*, §§ 1804(a)(4), 1805(a)(3), (c)(2)(A); of physical searches for purposes of obtaining foreign intelligence information under Title II of FISA, *id.*, §§ 1823(a)(4), 1825(a)(3), (c)(2)(A), and of targeting the communications of non-U.S. persons, and U.S. persons located abroad, under Title VII of FISA, *id.*, §§ 1881a(c)(1)(A), (e), (g)(2)(A)(ii), (i)(2)(C), (3), 1881b(b)(1)(D), (c)(1)(C), (3)(C), (5)(A), 1881c(b)(4), (c)(1)(C), (3)(C).

By directing minimization of the retention as well as the dissemination of U.S. person information, Congress intended that "information acquired, which does not relate to approved purposes in the minimization procedures, be destroyed." S. Rep. No. 95-701, 40 (1978), 1978 U.S.C.C.A.N. 3973, 4009; *see id.* at 50 (minimization procedures "should where possible include … requirements for the deletion of information obtained which does not relate to foreign intelligence purposes"). *See also In re Sealed Case*, 310 F.3d 717, 731 (F.I.S.C. Rev. 2002) ("[b]y minimizing *retention*, Congress intended that 'information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed where feasible'") (quoting H.R. Rep. No. 95-1283 at 56). As Congress explained when it enacted FISA in 1978 and has repeatedly re-affirmed, "[t]he minimization procedures of

[FISA] provide vital safeguards" for U.S. persons "who are not the authorized targets of surveillance." S. Rep. No. 95-701 at 39. *See also* S. Rep. No. 112-229, 19-20 (2012), 2012 WL 4450819 (noting the importance of minimization procedures to ensuring that the rights of U.S. persons are sufficiently protected when their communications are incidentally collected); S. Rep. No. 12-174, 3 (2012), 2012 WL 2052965 ("minimization procedures … serve to protect the privacy and civil liberties of U.S. persons"); S. Rep. No. 110-209 (2007), 2007 WL 5334390 ("minimization procedures … are essential to the protection of United States citizens and permanent residents"); *see* March 7 FISC Op. & Order at 4 ("Congress has sought to protect the privacy interests of United States persons by requiring the government to apply minimization procedures that restrict the retention of United States person information").

As the FISC recognized in initially denying the Government's request for relief from its destruction obligations, the records that would have to be preserved if Plaintiffs' request were granted are "voluminous," and contain U.S. person information. *Id.* at 5. Their retention for purposes of hypothetical future discovery in civil litigation would be "unrelated to the government's need to obtain, produce, and disseminate foreign intelligence information." *Id.* at 7. Although the data would be stored under conditions that would preclude access by NSA analysts for any purpose, *see* Gov't Mot. for Second Amendment to Primary Order, at 8, their continued retention as Plaintiffs request would nevertheless contravene an important public policy that lies at the foundation of the statutory scheme enacted by Congress to regulate domestic surveillance conducted by the Government for foreign intelligence purposes. This is all the more reason why the Plaintiffs must demonstrate that the foreseeable value of the data to their claims is so substantial as to justify preserving them in the face of the FISC's orders.

C. Plaintiffs Offer Little Explanation Regarding the Metadata's Benefit to Their Case To Justify Their Retention.

Apart from their meritless argument that the preservation order in *Jewel* already requires the preservation of metadata that the NSA would otherwise age off, Plaintiffs say little in their papers to explain the relevance of the data to these proceedings. The Government does not dispute the data's relevance, within the meaning of Federal Rule of Civil Procedure 26(b)(1), to

claims challenging FISC-authorized activities. Indeed, that is why the Government initially sought leave from the FISC to preserve them. But the question presented now, in light of the FISC's March 7 Opinion and Order, is whether the potential evidentiary value of the data to a determination of the parties' claims and defenses is so substantial as to outweigh the burdens on the NSA of preserving them, and the statutory policy underlying FISA's minimization provisions. *See* section I, *supra*. Plaintiffs offer little basis on which to conclude that is so.[15]

Plaintiffs first point out that proof of collection of records pertaining to their telephone communications are potentially relevant to the question of their standing to challenge the legality of the telephony metadata program under Section 215. Pls.' Br. at 11. Again, the Government does not contest the point that the data are relevant to the Section 215 cases, but the inquiry does not end there. Plaintiffs overlook the fact that even if metadata were destroyed for purposes of compliance with the FISC's five-year retention limit, the Government would still retain up to five years' worth of data at all times. Plaintiffs identify no reason to believe, assuming (hypothetically) that the NSA collected records of their calls more than five years ago, that it would not also have done so within the last five years. In other words, it stands to reason (or, at the very least, Plaintiffs have not shown why it would not) that if data destroyed to comply with the FISC's five-year retention limit contained records of Plaintiffs' calls, then so, too, would the much larger body of records the NSA would continue to maintain. Plaintiffs' need for metadata that NSA would otherwise age off in order to establish their standing to contest the lawfulness of the telephony metadata program is not substantiated on this record.

To the contrary, Plaintiffs themselves disclaim reliance on those data to establish their standing. *See* Pls.' Br. at 11 ("disagree[ing]" that "plaintiffs lack sufficient evidence that their

[15] Plaintiffs suggest that the Government already acknowledged to the FISC that "destruction of the telephone records would be inconsistent with it preservation obligations" in *First Unitarian*. Pls.' Br. at 10. That is an inaccurate characterization of the Government's position. The Government explained to the FISC that it sought leave to preserve the data because they were "potentially relevant" and therefore their destruction "*could* be inconsistent with the Government's preservation obligations in connection with civil litigation pending against it." Motion for Second Amendment to Primary Order at 2, 7 (emphasis added). For that reason the Government sought leave from the FISC, in effect, to put a "litigation hold" on the data. *Id.* at 7. But in the wake of the FISC's March 7 ruling, the question of whether the data *must* be preserved has been joined, and this Court must evaluate whether the data are of such importance to Plaintiffs' case as to justify the burdens that preserving the data would entail.

specific communications records were collected"). Even more telling, none of the other plaintiffs in the half-dozen other pending cases challenging the lawfulness of the telephony metadata program, *see* March 7 FISC Op. & Order at 5 n.4 (listing cases), have moved either in the courts where those cases are pending, or in the FISC, to prevent the destruction of the data as required by the FISC's orders. And that is so notwithstanding that the plaintiffs in these other cases were provided the same notice of the Government's intention to abide by the FISC's March 7 ruling that the Government provided to the Plaintiffs here. *See* ECF No. 85 in *First Unitarian*. Under these circumstances, while the metadata may be relevant in principle, Plaintiffs' demonstration of their practical value is, to say the least, not a powerful one.

In support of preserving the data Plaintiffs also refer to the fact that the relief sought in *Jewel* includes "an inventory of [Plaintiffs'] communications, records, or other information that was seized in violation of the Fourth Amendment." *Jewel* Complaint, Prayer for Relief, ¶ B. But for the reasons discussed above, *Jewel* has no bearing on whether any telephony metadata collected pursuant to FISC authorization under Section 215 should be preserved. Plaintiffs offer no explanation, moreover, as to the purpose of this relief. It is often the case in litigation alleging the unlawful acquisition and/or maintenance of information about an individual that a plaintiff will seek an inventory or accounting of the records in question as a means of ensuring their expungement should the plaintiff prevail. *See, e.g., Camfield v. City of Oklahoma City*, 248 F.3d 1214, 1234-35 (10th Cir. 2001); *Research Air, Inc. v. Kempthorne*, 589 F. Supp. 2d 1, 5-6 (D.D.C. 2008). If that is Plaintiffs' purpose here, *see Jewel* Complaint, Prayer for Relief, ¶ B (seeking "destruction of all copies of [Plaintiffs'] communications records" seized in violation of the Fourth Amendment), then Plaintiffs are in effect seeking to prevent the NSA from destroying at this time alleged records pertaining to their communications (that they contend the Government should not have acquired in the first place) so as to provide a means of overseeing their destruction at some indefinite time in the future. Under circumstances where the Government is obligated by multiple orders of the FISC to destroy all bulk telephony metadata

more than five years old, there is little if anything to be gained by mandating their retention for purposes of creating such an inventory.[16]

In the final analysis, this Court will have to determine if the Plaintiffs' showing of the metadata's relevance to *First Unitarian* justifies the burdens that preservation would impose, including the diversion of substantial resources from the accomplishment of the NSA's national security mission, and the retention of U.S. person information in derogation of the important public policy underlying FISA's minimization requirements. For its part, the Government stands prepared to act in accordance with the courts' determination of its paramount obligation under the circumstances. If this Court concludes that preservation of metadata that the NSA would otherwise age off is not required, then the Government will destroy them in accordance with its obligations under the FISC's orders. If the Court orders that the data be preserved, then the Government will seek leave to do so from the FISC, so that the NSA is not left in the "untenable position" of having to comply with "conflicting directives" from the courts. March 12 FISC Op. & Order at 4.

IV. THE GOVERNMENT DEFENDANTS DO NOT OBJECT TO PLAINTIFFS' REQUEST FOR A PRESERVATION ORDER IN *FIRST UNITARIAN*

The Government has no objection to the entry of Plaintiffs' proposed preservation order in *First Unitarian* (*see* ECF No. 90-1 in *First Unitarian*), which is identical to the order issued in *Jewel*. That said, it remains the Government's position that the preservation order in *Jewel* does not extend to metadata collected by the NSA pursuant to FISC orders issued under FISA, and that no such preservation obligation should be imposed in *First Unitarian* unless the Court determines that the burdens the preservation of the data would place on the NSA are justified by the value of the data to Plaintiffs' case. In all events, the Government's obligations regarding preservation of telephony metadata should be made clear, and the Government should not be left

[16] Although, as a general matter, the fact that documents or information are privileged does not absolve a party of an obligation to preserve them, it is nevertheless pertinent here that the data Plaintiffs are seeking to compel the Government to preserve are classified, and subject to the DNI's assertion of the state secret secrets privilege in *Jewel*. *See* Public Declaration of James R. Clapper, Director of National Intelligence (ECF No. 168), ¶¶ 2, 19(B) (asserting state secrets privilege over "information that would tend to confirm or deny that particular persons were targets of or subject to NSA intelligence activities"). In light of the Government's assertion of privilege over these data, it is all the more unlikely, as a practical matter, that these data will become evidence in this litigation on the question of Plaintiffs' standing, or any other.

in the position of having to comply with conflicting court orders regarding the preservation (or destruction) of telephony metadata that are subject to the FISC's five-year retention limit.

V. PLAINTIFFS' REQUEST FOR DISCLOSURE OF THE GOVERNMENT'S PRESERVATION EFFORTS

Throughout these cases, the Government has been as forthcoming as reasonably possible in litigation challenging the conduct of classified intelligence programs. The Government made detailed disclosures to the Court in the fall of 2007 about its preservation efforts in the only way it could given the classified nature of the activities at issue, further offering to address any questions the Court might have about those efforts in a classified setting. In 2014, when faced with civil suits challenging the collection of metadata under FISC orders, the Government went to the FISC and sought leave to retain the data that the FISC's orders required the Government to destroy because the Government thought the data were potentially relevant and thus their destruction "could be inconsistent" with the Government's preservation obligations in civil litigation. *See* Gov't Mot. for Second Amendment to Primary Order, FISC No. BR 14-01 (Feb. 25, 2014) at 2. Finally, when the FISC denied the Government's motion, the Government forbore from destroying the data immediately to give the plaintiffs in the civil cases an opportunity to seek relief in district court if they so desired. *See,e.g.,* Gvt. Defs.' Notice Regarding Order of the FISC (ECF No. 85 in *First Unitarian*) (filed Mar. 7, 2014). The Government has demonstrated its commitment to the preservation of relevant evidence with these actions.

Plaintiffs' request that the Government be required to disclose what it has done to comply with its preservation obligations and whether evidence has been destroyed is largely satisfied by the documents submitted herewith. As noted above, the Government is today providing now unclassified details about its compliance with this Court's preservation orders in *Jewel* and *Shubert*. The unclassified version of the Government's 2007 submission describes the categories of documents and information related to the presidentially-authorized activities that the Government has preserved, including Internet and telephony metadata. And the classified

declaration that the Government is filing herewith describes the Government's preservation efforts with respect to data collected under FISC authorization.[17]

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court reject Plaintiffs' request for an order "reaffirming" that the Government was required in *Jewel* and *Shubert* to preserve telephony metadata and other information acquired pursuant to FISC orders. In *First Unitarian*, the Government should not be required to preserve telephony metadata that the NSA otherwise would age off to comply with FISC orders unless this Court determines that the value of those data to Plaintiffs' case outweighs both the costs and burdens on the NSA of preserving them, and the policies underlying FISA's minimization requirements. The Government does not oppose the entry of a preservation order in *First Unitarian* akin to the order in *Jewel* so long it is otherwise consistent with the Government's positions in this submission. The Government is willing, if given sufficient time and if the Court desires, to make a further submission providing additional information regarding its preservation efforts relating to the NSA's collection of bulk telephony metadata under Section 215.

Dated: March 17, 2014

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director
tony.coppolino@usdoj.gov

[17] It was not possible, however, to compile detailed information setting forth the Government's preservation efforts with respect to other documents and information related to the FISC-authorized programs in the time available to submit this brief. The Government is willing, however, to submit a declaration describing those efforts if the Court so desires, but would require substantially more time than a mere fifteen days, to do so, particularly in light of the prospect that multiple declarations may be required. Furthermore, because the information necessary to describe these efforts may be classified in whole or in part, the Government may be required to submit much or all of it *in camera* and *ex parte* for the Court's consideration.

MARCIA BERMAN
Senior Trial Counsel

BRYAN DEARINGER
Trial Attorney

RODNEY PATTON
Trial Attorney

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

Attorneys for the Government Defendants Sued in their Official Capacities

EXHIBIT A

~~TOP SECRET//COMINT [redacted] //TSP//ORCON/NOFORN//MR~~

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates to: ALL CASES except *Al-Haramain v. Bush* (07-109); *CCR v. Bush* (07-1115); *United States v. Farber* (07-1324); *United States v. Adams* (07-1326); *United States v. Volz* (07-1396); *United States v. Gaw* (07-1242); *Clayton v. AT&T Communications of the Southwest* (07-1187)	MDL Dkt. No. 06-1791-VRW **CLASSIFIED DECLARATION OF [redacted] NATIONAL SECURITY AGENCY** **SUBMITTED *IN CAMERA, EX PARTE*** Hon. Vaughn R. Walker Date: November 15, 2007 Time: 2:00 pm Courtroom: 6 - 17th Floor

I, [redacted] do hereby state and declare as follows:

Introduction

1. **(U)** I am the Deputy Chief of Staff for Operations and Support for the Signals Intelligence Directorate of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I oversee signals intelligence (SIGINT) operations of NSA which includes the SIGINT units of the U.S. armed services. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), the NSA SIGINT Directorate is responsible for the collection, processing, and dissemination of SIGINT information for the foreign intelligence purposes of the United States. I am responsible for protecting NSA SIGINT activities, sources and methods against unauthorized disclosures. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995),

as amended on March 25, 2003, 68 Fed. Reg. 15315 (2003), and Department of Defense Directive No. 5200.1-R, Information Security Program Regulation, 32 C.F.R. § 159a.12 (2000). I have worked at NSA for thirty three years in various positions as a linguist, analyst and supervisor. As the Deputy Chief of Staff for Operations and Support, I am familiar with the document retention and preservation policies of the NSA.

2. ~~(TS//SI [redacted]//TSP//OC/NF)~~[1] I make this declaration in support the United States' Opposition to Plaintiffs' Motion for an Order to Preserve Evidence. The purpose of this declaration is to describe the policies and practices in place at NSA to preserve documents and information related to particular intelligence activities authorized by the President after the 9/11 attacks that are implicated by the claims in this proceeding, as well as to discuss steps that I understand have been taken [redacted]

3. ~~(TS//SI [redacted]//TSP//OC/NF)~~ I will address the following topics in this declaration. First, I briefly summarize the intelligence activities implicated by these lawsuits and which are subject to the Government's state secrets privilege assertion, as previously in described in the classified Declarations that Lt. General Keith T. Alexander, Director of NSA, has submitted in support of the United States' assertion of the state secrets privilege and NSA statutory privilege in *Hepting v. AT&T*, which involved claims against AT&T, and in the various cases against various *Verizon* defendants (hereafter "*In Camera* Alexander Declaration in *Hepting* Case or *Verizon* Cases"). Second, I identify categories of documents and information that may be related to these activities [redacted] Third, [redacted]

[1] **(U)** Classification markings in this declaration are in accordance with the marking system described in the *In Camera* Alexander Declarations submitted in the *Hepting* and *Verizon* cases.

[redacted] I then describe the specific preservation status of various categories of documents and information potentially relevant to this litigation.

4. (U) My statements in this declaration are based on my personal knowledge of NSA activities as well as information provided to me in the course of my official duties. I have become familiar with the subject matter of the lawsuits before the Court in this action and the Plaintiffs' pending motion. In particular, I have read the Plaintiffs' Motion as well as the classified declarations that General Alexander has submitted, *see supra* ¶ 3

5. ~~(TS//SI [redacted]//TSP//OC/NF)~~ In addition, the description set forth herein of the documents and information maintained and preserved [redacted] is known to and has been obtained by NSA in the course of its official duties. As previously described by General Alexander, NSA [redacted] in carrying out its signals intelligence mission. *See In Camera* Alexander Declaration in *Hepting* Case ¶¶ 3, 27-33; *In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 3-4, 24-26. [redacted]

Summary

6. ~~(TS//SI [redacted]//TSP//OC/NF)~~ NSA [redacted] taken affirmative steps (described below) to ensure the preservation of information that may be relevant to this litigation. In particular, NSA is preserving a range of documents and communications concerning the presidentially-authorized activities at issue, including: authorizations for these activities by the President; communications [redacted] documents related to the TSP, including specific selectors (*e.g.*, telephone numbers and email addresses) tasked for content interception and the reasons they were targeted; the actual content of communications intercepted under the TSP; intelligence reports containing TSP information; Internet and telephony metadata collected under the Presidential authorization; requests that NSA task that metadata for analysis to obtain information on terrorist contacts [redacted] and the reports of that analysis; and miscellaneous information concerning these activities, including legal opinions and analysis relating to the lawfulness of the TSP and metadata activities; briefing materials used to advise Members of Congress and the Foreign Intelligence Surveillance Court about these activities; internal NSA oversight materials, such as NSA Inspector General oversight of the operation of these activities; guidance used by NSA analysts concerning how to designate, use, and protect TSP information in intelligence reports; and technical information concerning the manner in which these presidentially-authorized activities were implemented, [redacted]

7. ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

[redacted]

Background

A. ~~(TS//SI//TSP//OC/NF)~~ NSA Activities

8. ~~(TS//SI [redacted]//TSP//OC/NF)~~ As General Alexander has previously described in detail, the lawsuits before the Court implicate several highly classified and critically important NSA intelligence activities [redacted]

As General Alexander explained, this information is subject to the Government's assertion of the state secrets and related statutory privileges and cannot be disclosed without causing exceptionally grave harm to national security. *See In Camera* Alexander Declaration in *Hepting* Case ¶¶ 27-78; *In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 23-90.

---

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

[3] ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

~~TOP SECRET//COMINT~~ [redacted] ~~TSP//ORCON/NOFORN//MR~~

9. ~~(TS//SI~~ [redacted] ~~TSP//OC/NF)~~ First, these lawsuits put at issue whether the NSA has intercepted the content of domestic communications of the plaintiffs and other U.S. citizens. As set forth in General Alexander's prior submissions, although the Plaintiffs wrongly allege that the NSA conducts a dragnet of surveillance of the content of millions of communications sent or received by people inside the United States, *see In Camera* Alexander Declaration in *Verizon* Cases at ¶ 54, [redacted] the NSA [redacted] the interception of the content of communications reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organizations pursuant to the President's Terrorist Surveillance Program ("TSP") [redacted]

10. ~~(TS//SI~~ [redacted] ~~TSP//OC/NF)~~ Second, again after the 9/11 attacks and pursuant to an authorization of the President, [redacted] the NSA [redacted] the bulk collection of non-content information *about* telephone calls and Internet communications (hereafter "metadata")—activities that enable the NSA to uncover the contacts [redacted] of members or agents of al Qaeda or affiliated terrorist organizations. Specifically, the President authorized the NSA to collect metadata related to *Internet* communications for the purpose of conducting targeted analysis to track al Qaeda-related networks. Internet metadata is header/router/addressing information, such as the "to," "from," "cc," and "bcc" lines, as opposed to the body or "re" lines, of a standard email. Since July 2004, the collection of Internet metadata has been conducted pursuant to an Order of the Foreign Intelligence Surveillance Court ("FISC") authorizing the use of a pen register and trap and trace device ("FISC Pen Register Order"). *See* 18 U.S.C. § 3127 (defining "pen register" and "trap and trace device").

11. ~~(TS//SI~~ [redacted] ~~TSP//OC/NF)~~ In addition, also after the 9/11 attacks,

[redacted] the NSA [redacted] the collection of *telephony* metadata conducted pursuant to an authorization of the President. Such metadata is compiled from call detail data [redacted] that reflects non-content information such as the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls. As with the broad Internet metadata collection now authorized by the FISA Court, the bulk collection of telephony metadata was and remains necessary to utilize sophisticated analytical tools for tracking the contacts [redacted] Since May 2006, [redacted] have been required to produce this information by order of the FISA Court ("FISC Telephone Records Order").

B. ~~(TS//SI//TSP//OC/NF)~~ Document Categories

12. ~~(TS//SI [redacted]//TSP//OC/NF)~~ I describe below the categories and preservation status of documents or information maintained by NSA [redacted] in the following three program activities prior to the relevant FISC Order for that activity:[4]

(i) The Terrorist Surveillance Program authorized by the President to intercept certain international communications into or out of the United States (*i.e.*,"one-end" foreign) that are reasonably believed to involve a member or agent of al Qaeda or affiliated terrorist organization; and

(ii) The collection of non-content data concerning Internet communications authorized by the President ("Internet metadata").

(iii) The collection of telephone calling record information ("telephony metadata") authorized by the President.

[4] ~~(TS//SI)~~ Because Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, this declaration does not address information collected pursuant to such an authorization or any retention policies associated therewith.

I cannot state that all documents and information concerning these activities have been preserved since the activities commenced under presidential authorization after the 9/11 attacks. I specifically describe below various categories of documents and information concerning these activities that may be potentially relevant to the litigation and that NSA [redacted] acted to preserve since the onset of this litigation.

~~(TS//SI//TSP//OC/NF)~~ Preservation of Information

A. ~~(TS/SI)~~ National Security Agency Information

13. ~~(TS//SI//TSP//OC/NF)~~ As set forth below, the NSA preserving documents and information potentially relevant to the claims and issues in this lawsuit with respect to the three categories of activities authorized by the President after 9/11 and detailed above for the period prior to the respective superseding FISC orders. NSA has taken various steps to ensure that staff and officials in offices that were cleared to possess information related to the presidentially authorized activities are preserving documents contained in their files and on their computer systems that relate to these activities. Initially, on January 10, 2006, the General Counsel of the National Security Agency, through a classified electronic mail communication, instructed that information, records, or materials (including in electronic form) related to the presidentially-authorized activities be preserved. Prior to the initiation of these lawsuits, NSA has held monthly internal meetings between the Office of General Counsel (OGC), Office of the inspector General, Signals Intelligence Directorate, and senior agency management, to discuss operational and logistical issues associated with the operation of the presidentially-authorized activities; the preservation of information and documents related to those activities has been regularly discussed at these meetings. Following the initiation of theses cases in 2006, NSA's OGC has used these meetings to regularly advise the relevant program offices to preserve all information related to these activities, including in electronic form. In addition, in August

2007, following the issuance of Congressional subpoenas for information related to the presidentially-authorized activities, NSA's OGC again instructed the NSA program officials and personnel who had been cleared for access to information concerning the pesidentially-authorized activities that all information and documents (including written or electronic) related to these activities and the current litigation be preserved. The categories of documents and information related to the presidentially authorized activities is described below.

1. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

14. ~~(TS//SI//TSP//OC/NF)~~ [redacted]

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

See In Camera Alexander Declaration in *Hepting* Case ¶¶ 61, 74-75; *In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 49-52; and *In Camera* Alexander Declaration in *Shubert* Cases ¶¶ 34-36. Pursuant to the presidential authorization, NSA analysts queried the collected metadata using telephone numbers and email addresses that are reasonably suspected to be associated with al Qaeda or a group affiliated with al Qaeda (as discussed above). [redacted]

[redacted] Also, as set forth below, NSA has preserved metadata collected in bulk [redacted] under presidential authorization.

2. ~~(TS//SI//TSP//OC/NF)~~ Presidential Authorizations

16. ~~(TS//SI//TSP//OC/NF)~~ NSA is preserving copies of all Presidential authorizations of the TSP and metadata collection activities described herein from the inception of these activities, including the periodic re-authorization of these activities by the President. These authorizations were accompanied by a current analysis of the terrorist threat facing the United States, and these threat memoranda have also been preserved. These documents originated outside of NSA and were obtained and are preserved solely in paper form. These documents are maintained in the offices of the NSA Director.

3. ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

17. ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

4. (U) Terrorist Surveillance Program Information

18. ~~(TS//SI//TSP//OC/NF)~~ NSA is preserving several categories of documents related to the Terrorist Surveillance Program under which the content of international, one-end foreign telephone and Internet communications reasonably believed to involve a member or

agent of al Qaeda or affiliated terrorist organization were intercepted during the existence of that program. These TSP documents include the following:

19. ~~(TS//SI//TSP//OC/NF)~~ TSP Tasking and Probable Cause Information: NSA is preserving documentation assembled by its analysts in the process of determining whether it should, in connection with the TSP, intercept the content of communications of a particular selector (*e.g.*, telephone number or email address). As set forth in General Alexander's prior declarations in this case, the interception of the content of communications under the TSP was triggered by a range of information, including sensitive foreign intelligence, obtained or derived from various sources indicating that a particular phone number or email address is reasonably believed by the U.S. Intelligence Community to be associated with a member or agent of al Qaeda or an affiliated terrorist organization. *See, e.g.*, *In Camera* Alexander Declaration in *Verizon* Cases ¶ 55. After NSA would task for content collection a particular phone number or email address that met this criteria, it preserved documentation of the particular selectors (telephone numbers and Internet addresses) and are reasons for the tasking. [redacted]

20. ~~(TS//SI//TSP//OC/NF)~~ [redacted] NSA preserves documentation on an electronic database of *telephony* selectors tasked (*i.e.*, telephone numbers reasonably believed to be associated with persons outside the United States). Since approximately September 2005, NSA has also maintained a record of foreign Internet selectors

in an electronic database (which includes the basis for tasking the selector). For the period prior to September 2005, tasking documentation identifying foreign Internet selectors is not complete. However, since the initiation of this lawsuit, NSA has acted to preserve all records that did exist at that time for foreign Internet tasking. [redacted]

21. ~~(TS//SI//TSP//OC/NF)~~ TSP Intercepted Content: As described herein, NSA is preserving the actual content of communications intercepted under the presidentially-authorized TSP as described in this paragraph. For voice intercepts under the TSP, NSA has maintained all "raw traffic" in an electronic database.[5] From the initiation of the TSP until the program ceased in 2007, the raw traffic of Internet content intercepts were maintained on a database for approximately 180 days. Because the operational relevance of this intelligence declined over time, and because the performance of this system is affected by the volume maintained on the online database, NSA migrated the raw Internet traffic to computer tape. However, NSA is preserving tapes of the Internet content intercepted under the TSP since the inception of the program.

22. ~~(TS//SI//TSP//OC/NF)~~ Intelligence Reports: NSA analysts have prepared detailed intelligence reports that utilize content intercepts obtained under the TSP authorization by the President. NSA intelligence reports are written assessments of intelligence on particular topics (for example, the threat of al Qaeda attacks or the activities of suspected al Qaeda operatives). For each of these reports, an NSA analyst is able to determine if information obtained through a TSP intercept was utilized. All NSA intelligence reports are preserved

---

[5] ~~(TS//SI//TSP//OC/NF)~~ Due to a technical malfunction (which occurred on or about January 26, 2007), raw telephony intercept for a period of approximately six months (June 2005-December 2005) was inadvertently deleted from this database. However, foreign intelligence information derived from these raw intercepts is preserved.

permanently in paper and electronic form.

5. ~~(TS//SI//TSP//OC/NF)~~ Internet and Telephony Metadata Collection

23. ~~(TS//SI [redacted]//TSP//OC/NF)~~ Internet Metadata Collection: As described above and in General Alexander's prior Declarations, starting in October 2001, and now pursuant to the FISC Pen Register Order, NSA has obtained [redacted] bulk metadata associated with electronic communications [redacted] *See, e.g., In Camera* Alexander Declaration in *Verizon* Cases, ¶ 31. NSA collected Internet metadata pursuant to Presidential authorization until [redacted] 2004 (nearly two years before these lawsuits commenced). On [redacted] 2004, NSA took initial steps to embargo this data from access by all NSA analysts. Because the Internet metadata collected prior to the FISC order was no longer being used for analysis, it was migrated to electronic tapes starting in January 2006. Those tapes are stored by the Signals Intelligence Directorate. To be clear, the presidentially authorized collection of internet metadata is segregated from information collected under the FISC Order of July 2004 and has not been destroyed.

24. ~~(TS//SI [redacted]//TSP//OC/NF)~~ Telephony Metadata Collection: As described above and in General Alexander's prior declarations, starting in October 2001, and now pursuant to the FISC Telephone Records Order entered in May 2006 (FISC Telephone Records Collection Order), NSA has collected [redacted] telephony metadata compiled from call detail records that [redacted] reflects non-content information such as the date, time, and duration of telephone calls, as well as the phone numbers used to place and receive the calls. *See, e.g.,*

In Camera Alexander Declaration in *Verizon* Cases ¶ 32. The telephony metadata NSA collected [redacted] prior to the FISC order is segregated in an online database from that collected after May 2006 under the FISC Order, but remains subject to querying for analysis of [redacted] contacts by those reasonably believed to be associated with al Qaeda and affiliated terrorist organizations.

25. ~~(TS//SI [redacted]//TSP//OC/NF)~~ For operational reasons, NSA maintains approximately five years worth of telephony metadata in its online database. Data acquired after 2003 under Presidential authorization is preserved electronically in an online data base. NSA has migrated to tapes telephony metadata collected during the period 2001-02, since the current operational relevance of that data has declined and continuing to maintain it on current operational systems would be unnecessary and would encumber current operations with more recent data. NSA's operational policy is to continue to migrate telephony metadata beyond five years old from an online database to tapes for preservation. To the extent NSA is required to halt the migration of older telephony metadata to tape, less relevant data would be retained in the operational system, encumbering the performance of the current online database because of the volume of data, and this would severely undermine NSA's ability to identify [redacted] contacts of suspected terrorist communications.

26. ~~(TS//SI//TSP//OC/NF)~~ Information Pertaining to Queries of Meta-Data: NSA is preserving documentation of requests that it query its database of Internet and telephony metadata for analysis. *See In Camera* Alexander Declaration in *Verizon* Cases ¶¶ 31-32 and *In Camera* Alexander Declaration in *Hepting* Cases ¶¶ 37-43 (describing contact chaining [redacted] of metadata). This documentation indicates the selectors (Internet addresses and phone numbers) that NSA searched in order to analyze particular contacts [redacted] for that selector, and the basis for its analysis for the selectors under which the

metadata was queried. Documentation of metadata queries is maintained by NSA's Signals Intelligence Directorate in electronic form.

27. ~~(TS//SI//TSP//OC/NF)~~ Reports of Metadata Analysis: NSA is preserving documentation of its analysis of Internet and Telephony Metadata obtained pursuant to Presidential authorization and prior to the respective FISC Orders for these activities. These reports include the results of any contact chaining [redacted] for particular selectors reasonably believed to be that of a member or agent of al Qaeda or affiliated terrorist organization. This documentation sets forth NSA's assessment of a particular Internet or telephony selector's contacts [redacted] in order to detect other potential al Qaeda associates. Reports documenting metadata analysis are maintained by NSA's Signals Intelligence Directorate in both an electronic database and in paper form.

6. ~~(TS/SI)~~ Miscellaneous NSA Information

28. ~~(TS//SI [redacted]//TSP//OC/NF)~~ As summarized below, NSA is also preserving miscellaneous categories of administrative records related to the presidentially-authorized activities implicated by these lawsuits (TSP content collection, Internet metadata collection, telephony metadata collection). These categories include:

(i) *Legal Opinions* and analysis relating to the lawfulness of the TSP and metadata activities. This information is maintained in paper form in the Office of the General Counsel.

(ii) *Materials Related to Briefings to Members of Congress and the FISA Court* on the TSP and metadata activities since their inception. These documents are being maintained and preserved in paper form by the Program Manager's Office for these NSA activities. In addition, an electronic version of the latest iteration of these briefings is also maintained. Although no briefing materials have been destroyed since the initiation of these lawsuits in 2006, it is possible that not all earlier iterations of briefings have been preserved.

(iii) *NSA Internal Oversight Documents* of the presidentially-authorized TSP and metadata collection activities, including reports by the NSA General Counsel and the NSA Inspector General of the operation of these activities. NSA also is preserving agendas and notes of regular monthly meetings between the Office of the General Counsel,

Office of the Inspector General, and the Signals Intelligence Directorate, which review and address legal and operational issues concerning the TSP and metadata collection activities described herein.

(iv) *Classification Guides* that address the classification status, processing, dissemination, and reporting of intelligence traffic and information obtained pursuant to the presidential authorization. This guidance, which NSA intelligence analysts use in analyzing TSP traffic, includes instructions on how to designate and protect TSP information in intelligence reports, how to designate its classification status, and how to implement NSA minimization procedures in drafting reports (typically procedures that require the minimization of the names of U.S. persons mentioned in such reports who are not foreign intelligence targets). This information is maintained in electronic form.

(v) *Technical Information* concerning the manner in which presidentially-Authorized activities were implemented, [redacted] such as technical proposals, and technical plans for undertaking particular tasks.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

* * *

54. (U) If the Court has any questions concerning this submission, the NSA is prepared to address them and assist the Court further through secure *in camera, ex parte*

proceedings.

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

DATE: 25 October 2007

[redacted]
Deputy Chief of Staff for Operations and Support
Signals Intelligence Directorate
National Security Agency

EXHIBIT B

PETER D. KEISLER
Assistant Attorney General
CARL J. NICHOLS
Deputy Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
ALEXANDER K. HAAS
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460

Attorneys for the United States

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	MDL Dkt. No. 06-1791-VRW
	CLASSIFIED SUPPLEMENTAL MEMORANDUM OF THE UNITED STATES IN OPPOSITION TO PLAINTIFFS' MOTION FOR ORDER TO PRESERVE EVIDENCE
This Document Relates to:	
ALL CASES except *Al-Haramain v. Bush* (07-109); *CCR v. Bush*, (07-1115); *United States v. Farber* (07-1324); *United States v. Adams* (07-1326); *United States v. Palmerino* (07-1326); *United States v. Volz* (07-1396)	**SUBMITTED *IN CAMERA*, *EX PARTE***
	Hon. Vaughn R. Walker
	Date: November 15, 2007 Time: 2:00 pm Courtroom: 6 - 17th Floor

INTRODUCTION

~~(TS//SI [redacted]//TSP//OC/NF)~~ The United States submits, for the Court's *in camera, ex parte* review, this supplemental classified memorandum and a classified declaration from the National Security Agency in further support of its opposition to Plaintiffs' Motion for an Order to Preserve Evidence. *See* Classified *In Camera, Ex Parte* Declaration of [redacted] Deputy Chief of Staff for Operations and Support, Signals Intelligence Division, National Security Agency.[1] This classified declaration describes the various steps taken by the NSA [redacted] to preserve certain documents and information related to particular intelligence activities authorized by the President after the 9/11 attacks, which may be potentially relevant to proving or disproving Plaintiffs' claims in these cases. This submission shows that the NSA [redacted] preserving a range of information related to these activities (even beyond what is likely potentially relevant). This submission also demonstrates that facts about specific information and information systems, and how the Plaintiffs' proposed order would effect them, are needed to address and adjudicate Plaintiffs' motion. And this submission also shows that Plaintiffs' proposed order, at the very least, would have an uncertain impact—and could impose serious harmful consequences—on an ongoing NSA activity that is directly implicated by the allegations in this case (the collection and analysis of telephony metadata). For this reason, and others set forth below and in our public opposition, entering such an order, in the face of the ample and appropriate preservation steps [redacted] would be ill-advised, and Plaintiffs' motion should be denied.

---

[1] ~~(TS//SI)~~ As set forth in our public opposition, the specific identify of [redacted] is withheld from the public record pursuant to Pub. L. 86-36, codified as a note to 50 U.S.C. § 402.

BACKGROUND

~~(TS//SI [redacted]//TSP//OC/NF)~~ As the United States has previously set forth in its prior classified submissions, the lawsuits before the Court implicate several highly classified and critically important NSA intelligence activities [redacted] *See In Camera* [redacted] Declaration ¶ 8. First, these lawsuits put at issue whether the NSA has intercepted the content of domestic communications of the Plaintiffs and other U.S. citizens. As we have previously demonstrated, Plaintiffs' allegation that NSA undertakes a "dragnet" surveillance on the content of millions of domestic communications is wrong. *See In Camera* Alexander Declaration in *Verizon* Cases at ¶ 54. Instead, [redacted] the Terrorist Surveillance Program, authorized by the President after the 9/11 attacks, under which international communications to or from the United States reasonably believed to involve a member or agent of al Qaeda or an affiliated terrorist organization were intercepted. *See In Camera* [redacted] Declaration ¶ 9.

~~(TS//SI [redacted]//TSP//OC/NF)~~ These lawsuits also allege that the Carrier Defendants have provided the NSA with all or, or substantially all, of their customers' call records. [redacted]

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

[redacted] Telephony metadata collection, like Internet metadata collection, supports a highly significant and ongoing intelligence method for analyzing and tracking terrorist communications, and thus cannot be disclosed without causing exceptionally grave harm to national security. *See id.*

~~(TS//SI [redacted]//TSP//OC/NF)~~ As the United States has also previously disclosed to the Court, all of the presidentially-authorized activities implicated by this litigation have been subject to subsequent authorizations under the Foreign Intelligence Surveillance Act. *See In Camera* [redacted] Declaration ¶¶ 9-11; *see also In Camera* Alexander Declaration in *Verizon* Cases, ¶¶ 28-32.[4]

~~(TS//SI [redacted]//TSP//OC/NF)~~ As summarized below and detailed in the *In Camera* [redacted] Declaration, the NSA [redacted] taken various steps to preserve certain documents and information concerning these presidentially-authorized activities at issue.[5]

---

[3] ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

[4] ~~(TS//SI//TSP//OC/NF)~~ Because Plaintiffs have not challenged activities occurring pursuant to an order of the FISC, the NSA classified submission does not address information collected pursuant to FISA authorization or any retention policies associated therewith. *See In Camera* [redacted] Declaration ¶ 12, n.4.

[5] ~~(TS//SI [redacted]//TSP//OC/NF)~~ [redacted]

~~TOP SECRET//COMINT [redacted] //TSP//ORCON/NOFORN//MR~~

SUMMARY OF INFORMATION PRESERVED

1. ~~(TS//SI//TSP//OC/NF)~~ NSA Information

~~(TS//SI//TSP//OC/NF)~~ The NSA is preserving the following categories of information concerning the presidentially-authorized activities that are implicated by Plaintiffs' claims:

(i) **Presidential Authorizations** for the TSP and metadata activities.

(ii) [redacted]

(iii) **Terrorist Surveillance Program** information including:

* *Specific Selectors* (e.g. telephone numbers and email addresses) tasked for content interception and the reasons they were targeted;

* *Actual Content* of communications intercepted under the TSP;

* *Intelligence Reports* that utilize TSP information;

(iv) **Internet and Telephony Metadata** collected under the Presidential authorization and related information including:

* *Tasking Requests* that NSA undertake metadata analysis to obtain information on terrorist contacts [redacted]

* *Reports of Metadata Analysis* of terrorist contacts [redacted]

(v) **Miscellaneous NSA Information** concerning the presidentially-authorized activities:

* *Legal Opinions* and analysis relating to the lawfulness of the activities;

* *Briefing Materials* used to advise Members of Congress and the Foreign Intelligence Surveillance Court about these activities;

* *NSA Oversight Materials*, such as NSA Inspector General oversight of the operation of these activities;

* *Classification Guidance* used by NSA analysts concerning how to designate, use, and protect TSP information in intelligence reports; and

---

[redacted]

* *Technical Information* concerning the manner in which these presidentially-authorized activities were implemented, [redacted] specifically to these activities.

See In Camera [redacted] Declaration ¶¶ 16-28.

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

ARGUMENT

~~(TS//SI [redacted] //TSP//OC/NF)~~ As the authority cited in the United States' public opposition indicates, Plaintiffs must demonstrate that there is an actual need for a preservation order, not simply an indefinite or unspecified possibility that information will be lost. *See* United States' Opposition to Plaintiffs' Motion for Order to Preserve Evidence ("USG Opp.") at 7-8 (citing *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 434-435 (W.D. Pa. 2004)). Courts have declined to enter such orders where adequate preservation steps have been taken. *See id.* at 436-37; *Treppel v. Bovail Corp.*, 233 F.R.D. 363, 370-72 (S.D.N.Y. 2006). Plaintiffs have failed to make any showing of the need for a preservation order and, in light of the state secrets privilege, their motion is necessarily based on a speculative

concerns that potentially relevant information is not being preserved.

~~(TS//SI [redacted] //TSP//OC/NF)~~ The NSA [redacted] legal obligations to preserve potentially relevant information and, were it not for the need to protect state secrets, would be able to show [redacted] preserving a wide range of such information, as set forth in the *In Camera* [redacted] Declaration. However, several specific factual issues concerning the documents and information possessed by the NSA [redacted] could not be discussed between the parties, and now make it impossible to adjudicate this motion. Such issues extend beyond the disclosure of whether specific carriers assisted the NSA on the particular activities at issue, or whether activities such as Internet and telephony metadata collection (and hence any relevant evidence about them) could be acknowledged. Even beyond these threshold problems to conferring about preservation issues, specific issues and uncertainties would arise in attempting to address the parties' preservation obligations and the impact of Plaintiffs' proposed order.

~~(TS//SI [redacted] //TSP//OC/NF)~~ For example, with respect to content surveillance, Plaintiffs challenge an alleged "content dragnet" that does not exist, *see In Camera* Alexander Declaration in *Verizon* Cases at ¶ 54, [redacted] But it is unclear whether, as a result, the NSA [redacted] need to preserve nothing concerning content surveillance, or whether [redacted] a wide range of information in order to prove there is no content dragnet. This is just one example of how imposing a blanket order to preserve potentially relevant evidence, without any meaningful discussion or specific adjudication as to what such an order should properly apply to, would create substantial uncertainty concerning the NSA's [redacted] preservation obligations.

~~(TS//SI//TSP//OC/NF)~~ Assuming information concerning the TSP were potentially relevant to Plaintiffs' content dragnet claim, precisely *what* information about this and the other presidentially-authorized activities would be subject to particular preservation requirements cannot be resolved. The NSA [redacted] preserving substantial operational information concerning the TSP and metadata activities (such as the identity of targeted selectors, intelligence reports and analysis, technical information concerning methods of TSP interception and metadata collection)—which may or may not be relevant to adjudicating the lawfulness of the activities [redacted] Certainly, not every document or communication within the NSA [redacted] related to carrying out the presidentially-authorized activities should necessarily be considered relevant to Plaintiffs' claims. But addressing which information and information systems may be potentially relevant, among the range of information and systems possessed by the NSA [redacted] would necessarily require the disclosure of classified operational details and intelligence sources and methods.

~~(TS//SI [redacted] //TSP//OC/NF)~~ Plaintiffs' proposed blanket order is not an appropriate solution and, indeed, could be potentially dangerous. As should be apparent from the *In Camera* [redacted] Declaration, the NSA [redacted] accumulated a substantial amount of information concerning the presidentially-authorized activities implicated by this litigation over the past six years, and Plaintiffs' proposed order would leave unresolved which of this information would be subject to preservation requirements. Plaintiffs' attempt to narrow the field of potentially relevant evidence serves only to heighten the uncertainty. [redacted]

[redacted]

[redacted] While this suggests that most, if not all, of the NSA's information concerning the presidentially-authorized activities need not be preserved, the Plaintiffs' proposed order would still apply to the United States as intervener, *see* Pls. Proposed Preservation Order at 2, and the precise scope of the order would remain unclear and unresolved since the parties cannot discuss nor litigate what the order does apply to or does not.

[redacted] But when faced with a Court order to take specific preservation steps as to unspecified information, clarity as to what those obligations entail is essential—particularly for an intelligence agency attempting to track the movement and activities of terrorists [redacted][6]

~~(TS//SI [redacted]//TSP//OC/NF)~~ Another example of the uncertainty—and potential harm—that would result from Plaintiffs' proposed order concerns the collection of telephony metadata. This appears to be the only presidentially-authorized activity that is directly at issue in this litigation. As set forth by NSA, telephony metadata collected under presidential authorization is being preserved by NSA and, thus, to the extent this includes information derived from Plaintiffs' telephone records, there should be no preservation concern warranting the imposition of a preservation order. *See In Camera* [redacted] Declaration ¶¶ 24-25. Of course,

---

[6] ~~(TS//SI//TSP//OC/NF)~~ Moreover, a determination of the impact of the state secrets privilege in these cases should precede the imposition of any preservation order. For example, because the alleged content dragnet does not exist and state secrets would be required to show that, and evidence required to establish or disprove Plaintiffs' standing cannot be disclosed, and the existence of metadata activities is properly protected, the issuance of any preservation injunction with respect to any of these activities would be inappropriate.

even this most basic fact could not be disclosed in order to confer with Plaintiffs about preservation obligations or to address this motion. And, unless expressly addressed, Plaintiffs' proposed blanket order could adversely impact ongoing NSA. Telephony metadata obtained by NSA [redacted] under presidential authorization remains in operational use at NSA and is subject to querying for analysis of [redacted] contacts in conjunction with data collected under the May 2006 FISC Telephone Records Order. *See In Camera* [redacted] Declaration ¶ 24. For operational reasons, NSA maintains approximately five years worth of telephony metadata in its online database (which would include data acquired after 2003 under Presidential authorization). *See id.* ¶ 25. NSA's operational policy is to migrate older telephony metadata to computer tape as its operational relevance declines, because continuing to maintain it on current operational systems would be unnecessary and would encumber the performance of the current online database in analyzing this data. *Id.* If NSA were required to halt this practice—which might or might not be required under the Plaintiffs' proposed order—it would severely undermine NSA's ability to identify [redacted] contacts of suspected terrorist communications. *See id.* ¶ 25 and Pls. Proposed Preservation Order ¶ 3 (which would require halting relocation of data or arranging for the preservation of complete and accurate copies). However, to even address the matter would require confirmation of the activity, disclosure of NSA's operational practices, and a discussion of the details of NSA's information systems, which is not possible here. Indeed, any discussion of the matter would also risk or require disclosure of the FISC Telephone Records Collection Order itself, to demonstrate an important limitation on the scope of potentially relevant evidence concerning telephony metadata. Thus, while NSA already appears to be preserving this information as Plaintiffs would wish, that cannot be confirmed or adjudicated, and an order should not be entered that would create any

doubt as to the matter.[7]

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

~~(TS//SI [redacted]//TSP//OC/NF)~~ Finally, to the extent Internet metadata collection is at issue in this case, that activity ceased under presidential authorization two years before this litigation commenced, [redacted] *See In Camera* [redacted] Declaration ¶¶ 36, 45. [redacted]

[redacted] NSA itself preserves the metadata collected prior to the July 2004 FISC Pen Register Order, but has migrated that information to computer tapes. *See id.* ¶ 23. This would seem to be a more than adequate preservation step to the extent Internet metadata collection is at issue in these cases, but in light of its highly classified nature, no information concerning the existence of

---

[7] ~~(TS//SI//TSP//OC/NF)~~ To the extent potentially relevant, NSA is preserving information preserving documentation of requests that it query its database of Internet and telephony metadata for analysis, and reports of metadata analysis. *See In Camera* [redacted] Declaration ¶¶ 26-27. [redacted]

this activity, [redacted] or how information related to Internet metadata collection is being preserved, could be addressed either in conferring with the Plaintiffs or adjudicating their motion. Indeed, any such discussion again would specifically risk or require disclosure of the FISC Pen Register Order to demonstrate an important limitation on the scope of potentially relevant evidence concerning Internet metadata.[8]

~~(TS//SI [redacted] //TSP//OC/NF)~~ These examples, which cannot be aired in our public opposition, illustrate the practical issues and complexity that arose in attempting to confer with Plaintiffs about a preservation order, and that would arise in attempting to adjudicate their motion. Accordingly, we submit that the Court should recognize that the Plaintiffs have not and cannot meet their burden of demonstrating the need for a preservation order and, light of the classified showing in the *In Camera* [redacted] Declaration, that the NSA [redacted] endeavoring to fulfill [redacted] preservation obligations and, thus, conclude that a preservation order should not be entered.

CONCLUSION

(U) For the foregoing reasons, and those set forth in the United States' public opposition, Plaintiffs' Motion for an Order to Preserve Evidence should be denied.

DATED: October 25, 2007

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

CARL J. NICHOLS
Deputy Assistant Attorney General

---

[8] ~~(TS//SI [redacted] //TSP//OC/NF)~~ [redacted]

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel

s/ Alexander K. Haas
ALEXANDER K. HAAS
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460

Attorneys for United States

STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
RODNEY PATTON
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460

Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

CAROLYN JEWEL, *et al.* Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.* Defendants.	No. 08-cv-4373-JSW
FIRST UNITARIAN CHURCH OF LOS ANGELES, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	No. 13-cv-3287-JSW **PUBLIC DECLARATION OF TERESA H. SHEA** Date: March 19, 2014 Time: 2:00 P.M. Courtroom: 11 – 19th Floor Judge Jeffrey S. White

I, Teresa H. Shea, do hereby state and declare as follows:

INTRODUCTION

1. I am the Director of the Signals Intelligence Directorate (SID) at the National Security Agency (NSA), an intelligence agency within the Department of Defense (DoD). I am responsible for, among other things, protecting NSA Signals Intelligence activities, sources, and methods against unauthorized disclosures. Under Executive Order No. 12333, 46 Fed. Reg. 59941 (1981), as amended on January 23, 2003, 68 Fed. Reg. 4075 (2003), and August 27, 2004, 69 Fed. Reg. 53593 (2004), and August 4, 2008, 73 Fed. Reg. 45325, the NSA is responsible for the collection, processing, and dissemination of Signals Intelligence information for foreign intelligence purposes of the United States. I have been designated an original TOP SECRET classification authority under Executive Order 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Directive No. 5200.1-R, Information Security Program (Feb. 24, 2012).

2. My statements herein are based upon my personal knowledge of Signals Intelligence collection and NSA operations, information available to me in my capacity as Signals Intelligence Director, and the advice of counsel.

PRESERVATION ISSUES RELATING TO THE COLLECTION, RETENTION, AND DESTRUCTION OF TELEPHONY METADATA PURSUANT TO FISC ORDERS

3. Under the "business records" provision of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1861, as enacted by section 215 of the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("Section 215"), the Foreign Intelligence Surveillance Court ("FISC"), upon application by the Federal Bureau of Investigation (FBI), may issue an order "for the production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism." 50 U.S.C. § 1861(a)(1). Since May 2006, the NSA has collected bulk telephony metadata ("data") pursuant to FISC orders directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of "call detail" records[1] created by the recipient providers for calls to, from, or

[1] Under the terms of the FISC's orders, among other things, these data include, as to each call, the telephone numbers that placed and received the call, and the date, time, and duration of a call. These data do not include the substantive content of any communication, or the name, address, or financial information of a subscriber.

wholly within the United States. Under the FISC's orders, the NSA's authority to continue collecting the data expires after approximately 90 days and must be renewed. The FISC has renewed the daily collection of these data approximately every 90 days since May 2006 based on applications from the FBI, supported by the NSA, showing that the production of these call detail records satisfies the requirements of Section 215. To protect U.S. person information the FISC's orders impose procedures to minimize access to, use, dissemination, and retention of the data consistent with the need to acquire, produce, and disseminate foreign intelligence information. Among these is the requirement to destroy all bulk telephony metadata obtained under the FISC's Section 215 orders within five years (60 months) of the data's collection.

4. Recognizing that data collected pursuant to the Section 215 program could be potentially relevant to, and subject to preservation obligations in, a number of cases challenging the legality of the program, including *First Unitarian Church of Los Angeles v.* NSA, No. 13-cv-3287-JSW, the Government filed a motion with the FISC in which it sought an amendment of the FISC's prior orders to allow the Government to maintain data, which would otherwise be destroyed in compliance with prior FISC orders, for the limited purpose of complying with any applicable preservation obligations in the civil actions challenging the legality of the program. As the Government informed the FISC, the NSA intended to preserve and/or store the data that would otherwise be destroyed in a format that precludes any access or use by NSA intelligence analysts for any purpose.

5. While the FISC denied the Government's motion without prejudice on March 7, 2014, the NSA is currently preserving data that would otherwise be destroyed in accordance with the FISC's five-year retention limit pursuant to this Court's order of March 10 and the FISC's subsequent order of March 12, 2014, in which it granted the Government temporary relief from its obligation to destroy the pertinent data pending resolution of the preservation issues raised by Plaintiffs in the above-captioned actions. NSA intelligence analysts do not and will not have access to any data that are otherwise subject to the FISC-imposed destruction requirement while the question of whether the data must be preserved for litigation purposes is being resolved.

(Nor would they have access to the data afterward if they are ordered to be preserved.).[2]

6. I have been informed that Plaintiffs in these actions have requested that the Government be required to preserve the "telephone records" that the NSA has collected under the FISC-authorized telephony metadata program. This request could be taken to mean either (i) targeted preservation of metadata collected under Section 215 that pertain only to the Plaintiffs' telephone calls, or (ii) mass retention of all the data that are more than five years old. Both tasks would impose significant financial burdens on the NSA, divert personnel and technological resources from performance of the NSA's national security mission, and present other issues as well.

7. I am unable to state with any degree of particularity the burdens, costs, and risks associated with either solution in this public declaration. I have set forth those details, to the extent practicable at this time, in my classified declaration submitted to the Court *ex parte, in camera*.

8. Any solution requiring preservation of records beyond the five-year retention limit, however, would impose substantial burdens on the NSA and would divert limited financial, technological, and personnel resources away from foreign intelligence mission requirements. While it is impossible to quantify the additional risks such a diversion of resources may pose to the national security, I deem such risks to be significant.

9. Moreover, the fact that there is no way to predict how long the lawsuits before this Court will continue, coupled with ever-changing mission requirements and systems, make it extremely difficult to estimate costs and to devise the most cost-effective data storage solution should this Court issue an order requiring preservation of data that would otherwise be subject to age-off.

10. That said, I will provide in this public declaration as much detail as I can regarding the issues, burdens, costs, and risks of complying with either a court order to preserve only the telephony metadata (if any) related to Plaintiffs' calls or a court order for mass

[2] By order of the FISC on March 12, 2014, NSA technical personnel may access the 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 business records metadata.

preservation of all bulk telephony metadata collected more than five years ago.

Targeted Preservation of Telephony Metadata Related to Plaintiffs' Calls

11. To the extent Plaintiffs seek targeted preservation of data associated only with their own telephone calls, the NSA first would have to determine whether it has ever collected data pursuant to Section 215 associated with Plaintiffs' calls. For the NSA to make this determination, each Plaintiff organization and each individual Plaintiff would have to provide the NSA with all telephone numbers they were assigned or used at any time during the period for which data that would otherwise be destroyed must be preserved. The Plaintiffs would also have to inform the NSA of the specific time period during which they were assigned or used each telephone number, so that data pertaining to the calls of other persons who may have used or been assigned a particular number are not inadvertently retained. For the same reason, if this litigation continues long enough, each Plaintiff would have to inform the Government of any changes in the numbers they use or are assigned.

12. To comply with any preservation order that required the retention of only telephony metadata associated with Plaintiffs' calls (if any), the NSA would not simply be preserving data consisting of the Plaintiffs' phone numbers; the preserved data would include, among other information, the initiating and receiving number, and the date, time, and duration of each call in each record that was collected. For example, if a call detail record concerning a phone call made by a Plaintiff collected, that Plaintiff's telephone number as well as the receiving number—which may be that of an individual not in any way associated with these lawsuits—would be preserved together, along with the date, time, and duration of that individual's call with the Plaintiff.

13. Moreover, pursuant to the FISC's orders, NSA intelligence analysts may not access the data except through queries conducted for foreign intelligence purposes using identifiers (e.g., telephone numbers) that are reasonably suspected of being associated with foreign terrorist organizations that have been approved for targeting by the FISC. Therefore, even if Plaintiffs were willing to provide the NSA with the telephone numbers that they used or were assigned during the relevant time period, to identify records of Plaintiffs' calls would

possibly require prohibited queries of the database for purposes other than obtaining foreign intelligence information by using identifiers (Plaintiffs' telephone numbers) that have not been approved under the "reasonable, articulable suspicion" standard. This means that, before determining whether the NSA has collected metadata associated with Plaintiffs' calls, the Government may first have to seek and obtain approval from the FISC to run queries in the NSA's database for records associated with each telephone number provided by each Plaintiff. In the event that data associated with any calls made by Plaintiffs have been collected by the NSA, the queries, among other things, will return—and, in accordance with any preservation obligation imposed by the Court, the NSA would separately maintain—a collection of records indicating the telephone numbers with which each Plaintiff was in contact over a period of one or more years, depending on how long the NSA must continue to preserve data it would otherwise destroy.

14. In addition to the foregoing considerations are the time, effort, and resources that would be required for the NSA to preserve until the conclusion of the litigation any metadata related to Plaintiffs' calls, if any were collected. As more fully explained in my classified declaration submitted *ex parte, in camera*, a court order for the retention of metadata pertaining only to Plaintiffs' calls (assuming such data have been collected) would require the NSA to devote significant financial and personnel resources over several months—assets that would otherwise be devoted to the NSA's national security mission—to create, test, and implement a solution that would preserve only these targeted data on an ongoing basis. Also, the NSA would have to take reasonable steps designed to ensure appropriate continued preservation and/or storage, as well as the continued integrity of the data so that the data would be accessible and retrievable for any possible discovery requests. Costs would greatly increase if the NSA were ever required to retrieve these data for litigation purposes.

Retention of All "Aged Off" Telephony Metadata for the Duration of the Litigation

15. The alternative to identifying, extracting, and preserving metadata pertaining only to Plaintiffs' telephone calls (if any were collected) would be to preserve all telephony metadata collected more than five years ago in a format that precludes any access or use by NSA personnel for any purpose other than ensuring continued compliance with the Government's

preservation obligations. Given that the FISC granted the Government only temporary relief from its destruction obligations pending resolution of the preservation issues in the above-captioned actions, the Government would be required to seek an order from the FISC that would allow the Government to retain all of the data that would otherwise be aged off for the duration of this litigation.

16. As discussed more fully in my classified declaration submitted by the Government *ex parte, in camera*, the amount of data involved is voluminous and would grow in size over time, depending on the duration of this litigation. Mass retention of this data, and thereafter making them accessible for possible discovery purposes, could require the diversion of significant financial, personnel, and technological resources from the pursuit of NSA's core national security mission. As with the alternative approach of preserving only metadata associated with Plaintiffs' calls (if any), the costs involved with implementing this approach would greatly increase if the NSA were ever required to retrieve these data for litigation purposes.

17. The NSA has essentially two options for mass retention of the data. Both involve significant software development costs to create the capability to transfer data from the operational database to the preservation medium as that data age off. The first option would thereafter place considerable burdens on the NSA's information technology and personnel resources that would remain ongoing, and in fact increase, as this litigation continues. The second option, while more cost-effective and less burdensome than the first option so far as preservation of the data are concerned, would require significant investments of time—up to several months—by NSA personnel and a corresponding investment of NSA technological resources to make the data accessible for any possible discovery purpose. Both the NSA personnel and the technological resources needed to access, retrieve, and render usable this preserved data would be diverted from the pursuit of the NSA's core mission of collecting, processing, and disseminating signals intelligence for national security purposes.

PRESERVATION OF OTHER POTENTIAL EVIDENCE

18. I understand that Plaintiffs have inquired what steps the Government has taken to preserve telephony metadata, Internet metadata, and communications content collected by the

NSA under authority of the President following the September 11, 2001, terrorist attacks, and thereafter under FISC authority pursuant to sections 402, 501, and 702 of FISA, as well as other documents and information pertaining to those activities.It is not feasible in the time available to respond to Plaintiffs' Opening Brief re: Evidence Preservation to describe in detail the various steps that the NSA has taken to preserve documents and information related to the bulk collection of Internet and telephony metadata, and the collection of communications content, under FISC authority pursuant to sections 402, and 702 of FISA. I have addressed those matters in my classified *ex parte, in camera* declaration to the extent practicable, given that Plaintiffs filed their brief at the close of business on Thursday March 12. What I can say in this public declaration follows. Nothing stated herein, however, is intended to be, or should be construed as, an admission that documents and information pertaining to activities carried out under FISC authority, including the data collected, are relevant to the *Jewel* litigation (or its companion case, *Shubert v. Obama*).

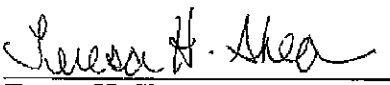
19. The steps taken by the Government to identify and to preserve documents and information related to the particular intelligence activities authorized by the President in the wake of the September 11 attacks are described in the Government's Classified Supplemental Memorandum in Opposition to the Plaintiff's Motion for Order to Preserve Evidence, dated October 25, 2007, filed in the case styled *In re NSA Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW. The Government supported its Memorandum with a classified *in Camera, Ex Parte* Declaration by an NSA official to apprise the Court of the preservation efforts that the Government had undertaken. A declassified version of the Government's memorandum and a declassified version of the declaration (both formerly provided to the Court for *ex parte, in camera* review) have been prepared for public filing in this litigation. As explained in the now declassified declaration, the NSA had at that time (2007) preserved, and the NSA continues to preserve, among other things, Internet and telephony metadata collected and the content of communications intercepted, under Presidential authority, in connection with the NSA intelligence programs known collectively as the President's Surveillance Program.

20. As discussed above, since the inception of the FISC-authorized bulk telephony

metadata program in 2006, the FISC's orders authorizing the NSA's bulk collection of telephony metadata under FISA Section 501 (known also as the Section 215 program) require that metadata obtained by the NSA under this authority be destroyed no later than five years after their collection. In 2011, the NSA began compliance with this requirement (when the first metadata collected under the FISC authority was ready to be aged off) and continued to comply with it until this Court's March 10 order and the subsequent March 12, 2014 order of the FISC. As a result, the NSA currently retains bulk telephony metadata collected under FISC authority dating back to 2009.

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

Executed on: March 17, 2014



Teresa H. Shea