

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

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

14 \_\_\_\_\_ )  
CAROLYN JEWEL, *et al.*, )  
15 Plaintiffs, )  
16 v. )  
17 NATIONAL SECURITY AGENCY, *et al.*, )  
18 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

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

1 **INTRODUCTION**

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

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

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

1 that the data may be deemed relevant to the plaintiffs' cases in the various suits challenging the  
2 program's lawfulness. On March 7, 2014, the FISC denied that request without prejudice,  
3 finding that preservation would be inconsistent with FISA's minimization requirements, at least  
4 on the record then before the court. However, following this Court's March 10 order directing  
5 that the data be preserved pending further instruction from this Court, the FISC on March 12,  
6 2014, granted the Government leave to retain the data pending resolution of the instant matter, in  
7 recognition that it is now necessary and appropriate for this Court to determine whether  
8 preservation of the data is required for purposes of this litigation.

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

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

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

1 the time the question of preservation was first litigated in the related multi-district litigation in  
2 2007, the Government specifically informed the Court of this limitation on the scope of  
3 potentially relevant evidence in a detailed classified filing before the Court entered its  
4 preservation order.<sup>1</sup> Thus, far from “conced[ing]” that information collected pursuant to FISC  
5 orders is relevant in *Jewel* and *Shubert*, as Plaintiffs contend, the Government has consistently  
6 hewed to its understanding of the *Jewel* Plaintiffs’ claims as challenging presidentially-  
7 authorized activity that occurred without court approval.

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

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

---

28 <sup>1</sup> A redacted, unclassified version of that declaration is filed herewith.

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

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

## 21 **BACKGROUND**

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

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

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

3 In *Jewel* and *Shubert*, Plaintiffs claim “that the federal government, with the assistance of  
4 major telecommunications companies, conducted widespread warrantless dragnet  
5 communications surveillance of United States citizens following the attacks of September 11,  
6 2001.” *Jewel v. NSA*, --- F. Supp. 2d ---, 2013 WL 3829405, at \* 2 (N.D. Cal. July 23, 2013).  
7 Of the two cases, *Shubert* was filed first, on May 17, 2006, and it was transferred to the *In re*  
8 *NSA Telecommunications Records Litigation* Multi-District Litigation (MDL) proceeding  
9 (designated as 3:06-md-1791-VRW (hereafter MDL-1791)). Joint Case Management Statement  
10 at 24 (ECF No. 159).<sup>2</sup> The *Jewel* complaint was filed on Sept. 18, 2008. *Id.* at 1. On Plaintiffs’  
11 motion, *Jewel* was related to *Hepting v. AT&T*, No. 06-cv-0672 (N.D. Cal.), the first case filed  
12 against telecommunications service providers for allegedly assisting in the alleged warrantless  
13 surveillance program, and the lead case in the MDL-1791 proceeding. *See* Admin. Motion by  
14 Plaintiffs to Consider Whether Cases Should be Related (ECF No. 7) (Pls.’ Mot. to Relate  
15 Cases); Plaintiffs’ Motion for a Temporary Restraining Order at 2 (Pls.’ Mot. for TRO) (ECF  
16 No. 186).

17 *Jewel* was brought by some of the same plaintiffs as in *Hepting*, but exclusively against  
18 the United States, its agencies, and current and former officials, whereas *Hepting* was against  
19 AT&T entities. Pls.’ Motion to Relate Cases at 2-3. Notably, as Plaintiffs’ motion to relate the  
20 cases expressly indicated: “both cases allege the same facts: that in 2001 the President  
21 authorized a program of domestic surveillance without court approval or other lawful  
22 authorization, and that through this Program, the government illegally obtains and continues to  
23 obtain with AT&T’s assistance the contents of Plaintiffs’ and class members’ telephone and  
24 internet communications, as well as records concerning those communications.” *Id.* at 3. *See*  
25 *also Jewel* Complaint at ¶ 7 (“In addition to eavesdropping on or reading specific  
26 communications, Defendants have indiscriminately intercepted the communications content and  
27  
28

---

<sup>2</sup> ECF numbers refer to filings in the *Jewel* case, unless otherwise indicated.

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

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

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

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

4 The declaration made clear, in a number of places, that the plaintiffs challenged activities  
5 that occurred under presidential authorization, not under orders of the Foreign Intelligence  
6 Surveillance Court (FISC), and that the declaration was therefore limited to describing  
7 information collected pursuant to presidential authorization and the retention thereof. In  
8 particular, the declaration stated that “[b]ecause Plaintiffs have not challenged activities  
9 occurring pursuant to an order of the FISC, this declaration does not address information  
10 collected pursuant to such an authorization or any retention policies associated therewith.”

11 Declass. NSA Decl. ¶ 12 n.4. The declaration also stated the following:

- 12 ■ “NSA is preserving a range of documents and communications concerning the  
13 presidentially-authorized activities at issue . . . .” *Id.* ¶ 6. The declaration described  
14 numerous categories of information being preserved, including Presidential  
15 authorizations, legal opinions and analysis, communications, content of  
16 communications intercepted under the TSP, intelligence reports containing TSP  
17 information, Internet and telephony metadata collected under the Presidential  
18 authorizations, reports of metadata analysis, briefing and oversight materials, and  
19 technical information. *Id.*
- 20 ■ The activities conducted pursuant to Presidential authorization—the interception of  
21 the content of communications reasonably believed to involve a member or agent of  
22 al Qaeda or an affiliated terrorist organization, the collection of Internet metadata, and  
23 the collection of telephony metadata—transitioned to FISC authorization. *Id.* ¶¶ 9-  
24 11.
- 25 ■ “I describe below the categories and preservation status of documents or information  
26 maintained by NSA [redacted] in the following three program activities prior to the  
27 relevant FISC Order for that activity: (i) The Terrorist Surveillance Program  
28 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

---

<sup>3</sup> 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.



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

5 ■ “To be clear, the presidentially authorized collection of internet metadata is  
6 segregated from information collected under the FISC Order of July 2004 and has not  
7 been destroyed.” *Id.* ¶ 23.

8 ■ “The telephony metadata NSA collected [redacted] prior to the FISC order is  
9 segregated in an online database from that collected after May 2006 under the FISC  
10 Order . . . .” *Id.* ¶ 24.

11 ■ “For operational reasons, NSA maintains approximately five years worth of  
12 telephony metadata in its online database. Data acquired after 2003 under  
13 Presidential authorization is preserved electronically in an online data base. NSA has  
14 migrated to tapes telephony metadata collected during the period 2001-02, since the  
15 current operational relevance of that data has declined and continuing to maintain it  
16 on current operational systems would be unnecessary and would encumber current  
17 operations with more recent data.” *Id.* ¶ 25.

18 ■ “NSA is preserving documentation of requests that it query its database of Internet  
19 and telephony metadata for analysis.” *Id.* ¶ 26.

20 ■ “NSA is preserving documentation of its analysis of Internet and telephony metadata  
21 obtained pursuant to Presidential authorization and prior to the respective FISC  
22 Orders for these activities.” *Id.* ¶ 27.

23 ■ “NSA is also preserving miscellaneous categories of administrative records related to  
24 the presidentially-authorized activities implicated by these lawsuits (TSP content  
25 collection, Internet metadata collection, telephony metadata collection).” *Id.* ¶ 28.

26 At the conclusion of the declaration, the Government offered to address any questions the Court  
27 may have had about the classified submission through secure *in camera*, *ex parte* proceedings.  
28 *Id.* ¶ 54.<sup>4</sup>

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

---

<sup>4</sup> 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.

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

10 On November 6, 2007, the Court entered a preservation order in the MDL litigation  
11 (which, again, included *Hepting*, the predecessor to *Jewel*, and *Shubert*). ECF No. 393 in MDL-  
12 1791. In that order, the Court reminded the parties of their duties to preserve evidence that may  
13 be relevant to the claims in the action. *Id.* at 2. The Court instructed that preservation includes  
14 taking “reasonable” steps to prevent the destruction of information “reasonably anticipated to be  
15 subject to discovery . . . .” *Id.* at 3. Then the Court directed counsel “to inquire of their  
16 respective clients if the business practices of any party involve the routine destruction . . . of such  
17 materials and, if so, direct the party, *to the extent practicable for the pendency of this order*,  
18 either to (1) halt such business processes; (2) sequester or remove such material from the  
19 business process; or (3) arrange for the preservation of complete and accurate duplicates or  
20 copies of such material, suitable for later discovery if requested.” *Id.* (emphasis added).

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

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

27 Following the unauthorized disclosure in June 2013 of a FISC order, issued on April 25,  
28 2013, which directed the production to the NSA of bulk call detail records, and the

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

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

27 <sup>5</sup> *See, e.g., American Civil Liberties Union v. Clapper*, No. 13-cv-3994 (WHP)  
28 (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.).

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

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

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

---

27  
28 <sup>6</sup> 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.

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

9         After receiving the FISC’s order, the Government began to notify the plaintiffs in *First*  
10 *Unitarian*, and other cases challenging the FISC authorized telephony metadata program, of the  
11 FISC’s March 7 order. Those notices stated that “[c]onsistent with that order, as of the morning  
12 of Tuesday, March 11, 2014, absent a contrary court order, the United States will commence  
13 complying with applicable FISC orders requiring the destruction of all call-detail records at this  
14 time.” Gvt. Defs.’ Notice Regarding Order of the FISC (ECF 85 in *First Unitarian*). On March  
15 10, plaintiffs in *First Unitarian*, *Jewel*, and *Shubert* moved for a temporary restraining order  
16 preventing the Government from destroying the call-detail records, which the Court granted that  
17 same day, pending further briefing. ECF No. 189.

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

1 **ARGUMENT**

2 **I. COMMON LAW PRESERVATION OBLIGATIONS IN CIVIL LITIGATION**

3 When litigation is reasonably anticipated against a party, that party has a common law  
4 obligation to preserve—i.e., identify, locate, and maintain—information that is “relevant to  
5 specific, predictable, and identifiable litigation.” *Apple Inc. v. Samsung Elec. Co., Ltd.*, 881 F.  
6 Supp. 2d 1132, 1137 (N.D. Cal. 2012). “It is well-established that the duty pertains only to  
7 relevant documents.” *Id.* (collecting cases). “Relevant” in this context means relevant for  
8 purposes of discovery, *see, e.g.*, Fed. R. Civ. P. 26(b)(1), 34(a)(1), including information that  
9 relates to the claims or defenses of any party, and that which is reasonably calculated to lead to  
10 the discovery of admissible evidence. *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779  
11 (2d Cir. 1999); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18, 220 (S.D.N.Y. 2003)  
12 (“*Zubulake IV*”).

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

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

1 1886353, at \*11-12 (N.D. Ill. May 23, 2012) (“A party fulfills its duty to preserve evidence if it  
2 acts reasonably.”). Determining whether preservation conduct is acceptable in a given case  
3 “depends on what is reasonable, and that in turn depends on whether what was done—or not  
4 done—was proportional to that case.” *Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp.  
5 2d 598, 613 (S.D. Tex. 2010); *see also Pippins v. KPMG LLP*, 279 F.R.D. 245, 255 (S.D.N.Y.  
6 2012) (explaining that this inquiry “depends heavily on the facts and circumstances of each case  
7 and cannot be reduced to a generalized checklist of what is acceptable or unacceptable”) (internal  
8 quotations omitted).

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

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

1 should be considered in the proportionality analysis.”).<sup>7</sup> For this reason, courts considering a  
2 party’s preservation obligations, including whether additional preservation measures are  
3 necessary, balance the burden of preserving certain information with the moving party’s showing  
4 of its relevance. *See, e.g., Young v. Facebook, Inc.*, 2010 WL 3564847, at \*1 (N.D. Cal. Sept.  
5 13, 2010); *Jardin v. Datallegro, Inc.*, 2008 WL 4104473, at \*1 (S.D. Cal. Sept. 3, 2008);  
6 *Columbia Pictures Indus. v. Bunnell*, 2007 WL 2080419, at \*4-6, 13 (C.D. Cal. May 29, 2007);  
7 *Donini Intern., SPA v. Satec, LLC*, 2006 WL 695546, at \*8 (S.D.N.Y. Mar. 16, 2006).

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

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

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

---

28 <sup>7</sup> *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).



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

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

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

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

---

22           <sup>8</sup> Although the existence of these activities has now been declassified, they were highly  
23 classified at the time the parties were litigating the preservation order in the MDL litigation and  
24 at the time the *Jewel* preservation order was entered, and have been until very recently. Thus,  
25 Plaintiffs’ suggestion that had the Government had any question about the scope of its  
26 preservation obligations and what specific documents it was supposed to preserve (which it did  
27 not, in light of the nature of the allegations in *Jewel*), it could have simply “pick[ed] up the  
28 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.

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

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

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

---

13 <sup>9</sup> It bears noting that the court hearing the preservation matter did not question the  
14 Government’s approach to preservation or instruct the Government to preserve information  
15 related to the FISC-authorized programs, which had been described by the Government to the  
16 court repeatedly in classified declarations in support of the state secrets privilege dating back to  
2006.

17 <sup>10</sup> *See, e.g., Hepting* Amended Complaint (Am. Cmplt.) at ¶ 2 (“This case challenges  
18 the legality of Defendants’ participation in a secret and illegal government program to intercept  
19 and analyze vast quantities of Americans’ telephone and Internet communications, surveillance  
20 done without the authorization of a court and in violation of federal electronic surveillance and  
21 telecommunications statutes, as well as the First and Fourth Amendments to the United States  
22 Constitution.”), ¶ 3 (“This surveillance program, purportedly authorized by the President at least  
23 as early as 2001 and primarily undertaken by the National Security Agency (“NSA”) without  
24 judicial review or approval, intercepts and analyzes the communications of millions of  
25 Americans.”); *Shubert* Second Amended Complaint (SAC), filed May 8, 2012, ¶ 2 (“Without the  
26 approval of Congress, without the approval of any court, and without notice to the American  
27 people, President George W. Bush authorized a secret program to spy upon millions of innocent  
28 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 . . .”).

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

7         Although the Plaintiffs in *Jewel* sued the Government, not telecommunications service  
8 providers, their complaint too is unmistakably about the presidentially-authorized intelligence  
9 activities allegedly conducted without a court order. *See, e.g., Jewel* Complaint at ¶ 7 (“In  
10 addition to eavesdropping on or reading specific communications, Defendants have  
11 indiscriminately intercepted the communications content and obtained the communications  
12 records of millions of ordinary Americans as part of the Program authorized by . . . President  
13 [Bush].”), ¶ 39 (President Bush “authoriz[ed] “a range of surveillance activities . . . without  
14 statutory authorization or court approval, including electronic surveillance of Americans’  
15 telephone and Internet communications (the ‘Program’)”), ¶ 76 (“Defendants’ above-described  
16 acquisition in cooperation with AT&T of . . . communications content and non-content  
17 information is done without judicial, statutory, or other lawful authorization, in violation of  
18 statutory and constitutional limitations, and in excess of statutory and constitutional authority.”),  
19 ¶ 92 (“Defendants’ above-described solicitation of the disclosure by AT&T of . . .  
20 communications records . . . is done without judicial, statutory, or other lawful authorization, in  
21 violation of statutory and constitutional limitations, and in excess of statutory and constitutional  
22 authority.”), ¶¶ 110, 120, 129, 138 (“Defendants have [acquired] . . . contents of  
23 communications, and records pertaining to . . . communications . . . without judicial, statutory, or  
24 other lawful authorization, in violation of statutory and constitutional limitations, and in excess  
25 of statutory and constitutional authority.”).

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

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

19         Accordingly, Plaintiffs’ effort to recast the *Jewel* Complaint as challenging FISC-  
20 authorized activities is nothing more than a post-hoc, unfounded attempt to rewrite their  
21 Complaint in order to create a preservation dispute in *Jewel* concerning previously classified  
22 matters. All of Plaintiffs’ specific contentions in support of this theory are meritless. Plaintiffs  
23 first point to the statement in their Rule 56(f) declaration that they intended to take discovery  
24 regarding the fact of carriers’ interception and disclosure of the communications and  
25 communications records of customers (Pls.’ Br. at 7). But that indicates nothing more than that  
26 they seek discovery concerning an allegation in the complaint that records were collected  
27 pursuant to presidential authorization in “the Program,” and does not remotely indicate Plaintiffs  
28

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

3 Plaintiffs also point to references to now declassified FISC activities wholly out of  
4 context in an effort to show their Complaint must challenge activities undertaken *with* judicial  
5 authority. Plaintiffs cite references they made to “post-FISC transition surveillance” in the Joint  
6 Case Management Statement filed by the parties on September 20, 2013 (ECF No. 159). Pls.’  
7 Br. at 7. But those references concern what Plaintiffs claim to be the Government’s official  
8 disclosures following the unauthorized disclosures that began in June 2013—the subject the joint  
9 statement was supposed to address—and which prompted the Court to require further briefing on  
10 the national security issues in this case. *See* Jt. Statement at 4-5. Nothing Plaintiffs said in the  
11 joint statement indicated they were now challenging FISC-authorized activities. Plaintiffs  
12 further argue that in the Government’s section of the joint statement, “rather than asserting its  
13 current, cramped claims about the scope of the *Jewel* claims, the government instead conceded  
14 that ‘Plaintiffs claim this alleged ‘dragnet’ surveillance included collection of the content of  
15 telephone and Internet communications as well as communications records.’ Pls.’ Br. at 7-8.  
16 Again, this wrenches a snippet of text out of context. In the immediately preceding sentence, the  
17 Government specifically referred to the activities authorized by President Bush. Jt. Statement at  
18 33 (“In the above-captioned *Jewel* and *Shubert* cases, Plaintiffs allege that, following the 9/11  
19 terrorist attacks, then-President George W. Bush authorized the National Security Agency (NSA)  
20 to undertake, with the assistance of major telecommunications companies, indiscriminate  
21 warrantless surveillance of the communications of millions of Americans.”). Nothing stated by  
22 the Government remotely concedes that the *Jewel* Complaint challenges judicially-authorized  
23 FISC activities.

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

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

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

22 While the plaintiffs’ allegations are focused on the period immediately  
23 following 9/11, and seek to challenge alleged activities undertaken pursuant to  
24 presidential authorization, the sources and methods used by NSA at that time  
25 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

---

26 <sup>11</sup> *See also* United States’ Reply in Support of Mot. to Dismiss or, in the Alternative, for  
27 Summ. Judgment (ECF No. 520 in MDL-1791) at 32 n.29 (“All of the claims in this litigation  
28 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.

1 compromise, if not destroy, NSA's ability to use that method today. All of the  
2 presidentially authorized activities being challenged in this lawsuit (starting in  
3 July 2004) were placed under other FISA authority and have been subject to  
4 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.

5 2012 NSA Decl. ¶ 52. *See also id.* ¶¶ 7, 34, 37, 84; 2007 DNI Decl. ¶ 3; 2007 NSA Decl. 62-64;  
6 2009 DNI Decl. ¶ 40-41; 2009 NSA Decl. ¶¶ 26-27, 57- 67; 2012 DNI Decl. ¶ 56-57.

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

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



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

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

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

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

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

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

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

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

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

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

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

---

25 <sup>12</sup> The leave the FISC has temporarily granted the NSA to access the metadata for civil  
26 litigation purposes expires upon “resolution of the preservation issues” presented here. March 12  
FISC Op. & Order at 6-7.

27 <sup>13</sup> The Government would need to seek such approval, notwithstanding the FISC’s recent  
28 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.

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

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

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

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

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

28          <sup>14</sup> 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*.

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

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

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

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

5 The imposition of detailed minimization procedures limiting the retention and  
6 dissemination of information pertaining to U.S. persons for purposes other than foreign  
7 intelligence is not peculiar to Section 215. Minimization procedures are an essential feature of  
8 FISA’s statutory scheme. The Government’s adoption and the FISC’s approval and enforcement  
9 of specific minimization procedures “that are reasonably designed in light of the purpose and  
10 technique of the particular surveillance, to minimize the acquisition and retention, and prohibit  
11 the dissemination” of information concerning U.S. persons “consistent with the need of the  
12 United States to obtain, produce, and disseminate foreign intelligence information,” 50 U.S.C.  
13 § 1801(h)(1), are also statutory pre-requisites to the authorization of electronic surveillance  
14 under Title I of FISA, *id.*, §§ 1804(a)(4), 1805(a)(3), (c)(2)(A); of physical searches for purposes  
15 of obtaining foreign intelligence information under Title II of FISA, *id.*, §§ 1823(a)(4),  
16 1825(a)(3), (c)(2)(A), and of targeting the communications of non-U.S. persons, and U.S.  
17 persons located abroad, under Title VII of FISA, *id.*, §§ 1881a(c)(1)(A), (e), (g)(2)(A)(ii),  
18 (i)(2)(C), (3), 1881b(b)(1)(D), (c)(1)(C), (3)(C), (5)(A), 1881c(b)(4), (c)(1)(C), (3)(C).

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

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

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

23 **C. Plaintiffs Offer Little Explanation Regarding the Metadata’s Benefit to**  
24 **Their Case To Justify Their Retention.**

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



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

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

21 To the contrary, Plaintiffs themselves disclaim reliance on those data to establish their  
22 standing. *See* Pls.' Br. at 11 ("disagree[ing]" that "plaintiffs lack sufficient evidence that their  
23

---

24 <sup>15</sup> Plaintiffs suggest that the Government already acknowledged to the FISC that  
25 "destruction of the telephone records would be inconsistent with its preservation obligations" in  
26 *First Unitarian*. Pls.' Br. at 10. That is an inaccurate characterization of the Government's  
27 position. The Government explained to the FISC that it sought leave to preserve the data  
28 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.

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

10 In support of preserving the data Plaintiffs also refer to the fact that the relief sought in  
11 *Jewel* includes “an inventory of [Plaintiffs’] communications, records, or other information that  
12 was seized in violation of the Fourth Amendment.” *Jewel* Complaint, Prayer for Relief, ¶ B.  
13 But for the reasons discussed above, *Jewel* has no bearing on whether any telephony metadata  
14 collected pursuant to FISC authorization under Section 215 should be preserved. Plaintiffs offer  
15 no explanation, moreover, as to the purpose of this relief. It is often the case in litigation  
16 alleging the unlawful acquisition and/or maintenance of information about an individual that a  
17 plaintiff will seek an inventory or accounting of the records in question as a means of ensuring  
18 their expungement should the plaintiff prevail. *See, e.g., Camfield v. City of Oklahoma City*, 248  
19 F.3d 1214, 1234-35 (10th Cir. 2001); *Research Air, Inc. v. Kempthorne*, 589 F. Supp. 2d 1, 5-6  
20 (D.D.C. 2008). If that is Plaintiffs’ purpose here, *see Jewel* Complaint, Prayer for Relief, ¶ B  
21 (seeking “destruction of all copies of [Plaintiffs’] communications records” seized in violation of  
22 the Fourth Amendment), then Plaintiffs are in effect seeking to prevent the NSA from destroying  
23 at this time alleged records pertaining to their communications (that they contend the  
24 Government should not have acquired in the first place) so as to provide a means of overseeing  
25 their destruction at some indefinite time in the future. Under circumstances where the  
26 Government is obligated by multiple orders of the FISC to destroy all bulk telephony metadata  
27  
28

1 more than five years old, there is little if anything to be gained by mandating their retention for  
2 purposes of creating such an inventory.<sup>16</sup>

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

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

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

---

25 <sup>16</sup> Although, as a general matter, the fact that documents or information are privileged  
26 does not absolve a party of an obligation to preserve them, it is nevertheless pertinent here that  
27 the data Plaintiffs are seeking to compel the Government to preserve are classified, and subject to  
28 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.

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

3 **V. PLAINTIFFS’ REQUEST FOR DISCLOSURE OF THE GOVERNMENT’S**  
4 **PRESERVATION EFFORTS**

5 Throughout these cases, the Government has been as forthcoming as reasonably possible  
6 in litigation challenging the conduct of classified intelligence programs. The Government made  
7 detailed disclosures to the Court in the fall of 2007 about its preservation efforts in the only way  
8 it could given the classified nature of the activities at issue, further offering to address any  
9 questions the Court might have about those efforts in a classified setting. In 2014, when faced  
10 with civil suits challenging the collection of metadata under FISC orders, the Government went  
11 to the FISC and sought leave to retain the data that the FISC’s orders required the Government to  
12 destroy because the Government thought the data were potentially relevant and thus their  
13 destruction “could be inconsistent” with the Government’s preservation obligations in civil  
14 litigation. *See* Gov’t Mot. for Second Amendment to Primary Order, FISC No. BR 14-01 (Feb.  
15 25, 2014) at 2. Finally, when the FISC denied the Government’s motion, the Government  
16 forbore from destroying the data immediately to give the plaintiffs in the civil cases an  
17 opportunity to seek relief in district court if they so desired. *See, e.g.*, Gvt. Defs.’ Notice  
18 Regarding Order of the FISC (ECF No. 85 in *First Unitarian*) (filed Mar. 7, 2014). The  
19 Government has demonstrated its commitment to the preservation of relevant evidence with  
20 these actions.

21 Plaintiffs’ request that the Government be required to disclose what it has done to comply  
22 with its preservation obligations and whether evidence has been destroyed is largely satisfied by  
23 the documents submitted herewith. As noted above, the Government is today providing now  
24 unclassified details about its compliance with this Court’s preservation orders in *Jewel* and  
25 *Shubert*. The unclassified version of the Government’s 2007 submission describes the categories  
26 of documents and information related to the presidentially-authorized activities that the  
27 Government has preserved, including Internet and telephony metadata. And the classified  
28

1 declaration that the Government is filing herewith describes the Government's preservation  
2 efforts with respect to data collected under FISC authorization.<sup>17</sup>

3 **CONCLUSION**

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

16 Dated: March 17, 2014

17  
18 Respectfully submitted,

19 STUART F. DELERY  
20 Assistant Attorney General

21 JOSEPH H. HUNT  
22 Director, Federal Programs Branch

23 ANTHONY J. COPPOLINO  
24 Deputy Branch Director  
[tony.coppolino@usdoj.gov](mailto:tony.coppolino@usdoj.gov)

---

25 <sup>17</sup> It was not possible, however, to compile detailed information setting forth the  
26 Government's preservation efforts with respect to other documents and information related to the  
27 FISC-authorized programs in the time available to submit this brief. The Government is willing,  
28 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.

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

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](mailto: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*