

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
 5 MARCIA BERMAN
 Senior Trial Counsel
 6 BRYAN DEARINGER
 Trial Attorney
 7 RODNEY PATTON
 Trial Attorney
 8 JULIA BERMAN
 Trial Attorney
 9 U.S. Department of Justice, Civil Division
 20 Massachusetts Avenue, NW, Rm. 7346
 10 Washington, D.C. 20001
 Phone: (202) 514-4782; Fax: (202) 616-8470

11 *Attorneys for the Government Defendants*
 12 *in their Official Capacity*

13 **UNITED STATES DISTRICT COURT**
 14 **NORTHERN DISTRICT OF CALIFORNIA**
OAKLAND DIVISION

15	CAROLYN JEWEL, <i>et al.</i> ,)
16)
17	Plaintiffs,)
18	v.)
19	NATIONAL SECURITY AGENCY, <i>et al.</i> ,)
20	Defendants.)

Case No. 4:08-cv-4373-JSW

**OPPOSITION TO PLAINTIFFS’
 EMERGENCY APPLICATION TO
 ENFORCE COURT’S TEMPORARY
 RESTRAINING ORDER**

Date: June 6, 2014
 Time: 2:00 p.m.
 Courtroom 5, 2nd Floor
 The Honorable Jeffrey S. White

22
 23
 24
 25
 26
 27
 28

INTRODUCTION

1
2 Assuming that the Court's June 5, 2014 order requires an immediate halt to destruction of
3 all Section 702 materials, that order creates an extremely significant operational crisis for the
4 National Security Agency. As set forth in the accompanying declaration of Richard H. Ledgett,
5 Deputy Director of the NSA ("Ledgett Decl.") (attached hereto as Exhibit A), it may not be
6 possible to comply immediately or in the near term with the Court's order without shutting down
7 all systems and databases that collect and store Section 702 communications data, which will
8 have enormous adverse consequences for NSA's ability to perform its foreign intelligence
9 mission. In the long term, NSA could not comply with this preservation mandate without
10 violating Foreign Intelligence Surveillance Court (FISC)-ordered minimization procedures that
11 are essential to the program's compliance with statutory and constitutional requirements, and
12 without potentially severe operational difficulties that could jeopardize national security.

13 The Court entered its order without hearing from the Government. In this brief, we
14 attempt to correct some of the misimpressions underlying Plaintiffs' filings, and consequently
15 the Court's order, and to persuade the Court to vacate its June 5 order. First, the preservation of
16 information acquired pursuant to Section 702 is far more complex and fraught with legal,
17 technical, and operational difficulties than the preservation of the Section 215 telephony
18 metadata. Unlike the Section 215 telephony metadata program, which resides on a discrete
19 computer systems architecture, communications acquired pursuant to Section 702 reside within
20 multiple databases contained on multiple systems. Those databases and systems are designed to
21 effectuate FISC-approved minimization procedures that require (with certain limitations) the
22 destruction (purge) upon recognition of certain communications and the age-off of certain raw
23 data within either two years or five years from the expiration of the certification authorizing its
24 acquisition. Halting these purges and age-offs to preserve all Section 702 material, as we
25 understand the Court to have ordered, would require significant technical changes to these
26 databases and systems and would have the effect of forcing NSA into non-compliance with
27 FISC-approved minimization procedures, thus placing the entire program in legal jeopardy.

1 Thus, far from maintaining the status quo, ordering the preservation of all Section 702 materials
2 requires the reconfiguration of the software and hardware used in these databases and systems.

3 Changes of this magnitude to database and systems architecture normally take months to
4 engineer and test; to comply immediately with the Court's order, the NSA may have to shut
5 down all the databases and systems that contain Section 702 information. Such a shutdown
6 would suspend acquisition of communications pursuant to Section 702 and analyst access to
7 communications acquired under Section 702. NSA would lose access to what would be
8 otherwise lawfully collected signals intelligence information on foreign intelligence targets that
9 are vital to the performance of NSA's foreign intelligence mission. Section 702 is the most
10 significant tool in NSA's arsenal for detecting, identifying, and disrupting terrorist threats to the
11 United States and around the world. The impact of a shutdown of the databases and systems that
12 contain Section 702 information cannot be overstated.

13 Second, the Temporary Restraining Order Plaintiffs seek to enforce (ECF No. 189) did
14 not expressly apply to Section 702 materials, nor did the context in which it was entered involve
15 Section 702 materials. Rather, the TRO was intended to prevent the destruction of Section 215
16 telephony metadata that was scheduled to age-off pursuant to retention limitations imposed by
17 the Foreign Intelligence Surveillance Court as a condition for its collection.

18 Third, the parties are in the middle of briefing whether this case implicates Section 702 at
19 all. Plaintiffs' complaints do not challenge Section 702 activity, which was public when
20 Plaintiffs filed their complaints, and to find that they challenge FISC-authorized activity would
21 be to invert their central claim against unauthorized activity. Moreover, it is highly unlikely that
22 any of Plaintiffs' communications have been acquired under Section 702. The statute authorizes
23 only targeted surveillance of non-U.S. persons located overseas; it is not a bulk collection
24 program like the Section 215 telephony metadata program (another reason why it does not fit
25 within Plaintiffs' claims of dragnet surveillance). It is also pure speculation as to whether
26 Plaintiffs' communications have been caught up in any incidental overcollection that has
27 occurred under the program, and illogical to suspend the very FISC requirements designed to
28 protect against this.

1 For all of these reasons, it would be a gross distortion of the Government's preservation
2 obligations to require it to preserve all Section 702 material for purposes of this litigation.

3 **BACKGROUND**

4 The March 10, 2014 Temporary Restraining Order

5 The dispute regarding the scope of the Government Defendants' preservation obligations
6 arose in the above-captioned cases after the Government confirmed the authenticity of an
7 unlawfully-disclosed Secondary Order of the FISC directing the production to the NSA of bulk
8 call detail records under Section 215 of the USA Patriot Act. Following that disclosure and
9 confirmation, several plaintiffs filed new suits challenging the legality of the Government's
10 acquisition of bulk telephony metadata under Section 215. *See, e.g., First Unitarian v. NSA*, No.
11 3:13-cv-3287(JSW) (N.D. Cal.). To enable the Government to preserve information that may be
12 relevant to those cases, in February 2014, the Government sought relief from the FISC
13 requirement that telephony metadata acquired under Section 215 be destroyed after five years.¹

14 Citing the Government's filing before the FISC, Plaintiffs emailed the Government
15 Defendants seeking "specific reaffirmation that bulk telephone records collected by the NSA
16 have been preserved in the *Jewel* case." ECF No. 186, Exh. E at 7. Plaintiffs then sought a
17 temporary restraining order "prohibiting . . . [the Government Defendants] from destroying any
18 evidence relevant to the claims at issue in this action, including but not limited to prohibiting the
19 destruction of any telephony metadata or 'call detail' records." *Id.* at 1.² On March 10, 2014,
20
21

22 ¹ The Government Defendants' Brief Regarding Compliance with Preservation Orders,
23 at 2-9 (ECF No. 229), further details the background related to this dispute.

24 ² Although Plaintiffs' motion for a temporary restraining order claimed that "[t]here
25 has been litigation challenging the lawfulness of the government's telephone metadata collection
26 activity, Internet metadata collection activity, and upstream collection activity pending in the
27 Northern District of California continuously since 2006," ECF No. 186 at 2, Plaintiffs provide no
28 citation or support for that contention. In reality, the claims in *Jewel* and *Shubert*, and the
balance of the MDL litigation, were directed only at presidentially-authorized NSA intelligence
activities, unauthorized by a court order. *See* Gov't Defs.' Brief Regarding Compliance with
Preservation Orders at 13-26 (ECF No. 229) (explaining that Plaintiffs did not, until the current
preservation dispute, purport to challenge any FISC-authorized intelligence gathering programs).

1 this Court issued a temporary restraining order containing the above-quoted language, and, *inter*
2 *alia*, setting a hearing for March 19, 2014 to address the issue further. ECF No. 189 at 2.

3 At the March 19, 2014 hearing, the Government Defendants noted that “the concern”
4 before the Court “[was] the telephony metadata that were subject to the age-off requirements
5 under the FISC’s orders.” Am. Tr. of Proceedings 7:22–24 (Mar. 19, 2014) (attached hereto as
6 Exhibit B). The Court agreed: “That’s correct. . . . and the occasion, of course, for the Court’s
7 issuing of the Temporary Restraining Order plus having [the March 19, 2014 hearing] is because
8 of the potentially imminent threat that these documents or this metadata would be destroyed
9 pursuant to federal statute.” *Id.* at 7:25–8:4.

10 At the same hearing, the Court rejected Plaintiffs’ request that the Government
11 Defendants, within 15 days, “disclose whether they have destroyed telephone records, Internet
12 metadata records, Internet or telephone content data, or any other evidence potentially relevant to
13 these lawsuits since the commencement of *Hepting, et al. v. AT&T et al.* litigation (No. 06-cv-
14 0672) in January 2006.” *See id.* at 91:16–17 (rejecting Paragraph 4 of Plaintiffs’ proposed
15 preservation order, ECF No. 191-1). Indeed, the Court specifically refused to order preservation
16 of “telephone records, Internet metadata records, Internet or telephone content data without
17 regard to when the government obtained them or the legal authority under which the government
18 obtained them,” *see id.* at 91:18–24 (rejecting Paragraph 1 of Plaintiffs’ proposed preservation
19 order, ECF No. 191-1), because this requirement was “too broad” and “the Plaintiffs’ suggested
20 language on the scope of materials to be preserved [was] not sufficiently tethered to their
21 Complaint.” *Id.* at 91: 18–19, 22–24. The Court then specifically directed, in the context of
22 addressing the preservation order for *First Unitarian*, that preservation obligations should extend
23 no farther than “the evidence that relates to the precise claims made by Plaintiffs in [their]
24 complaint.” *Id.* at 91:24–92:2.

25 Finally, at the conclusion of that hearing, the Court instructed the Government to brief its
26 compliance with the preservation order issued in *Jewel*. *Id.* at 92: 9–17.

1 The Current Dispute

2 Pursuant to this Court's March 19, 2014 order in *Jewel* and the *Shubert* Plaintiffs'
3 unopposed request that the same briefing also address compliance with this Court's preservation
4 order in *Shubert*, see *Shubert* ECF No. 117, the parties are currently briefing the scope of the
5 Government's preservation obligations in *Jewel* and *Shubert*. The Government Defendants
6 submitted their opening brief on these issues on May 9, 2014. See ECF No. 229.

7 While the *Jewel* Plaintiffs responded on May 30, 2014, ECF No. 233, the *Shubert*
8 Plaintiffs requested a 6-day extension. See Email Exchange among Counsel (attached hereto as
9 Exhibit C) at 4. The Government Defendants consented to this request, provided they could
10 address the *Shubert* and *Jewel* Plaintiffs' submissions in a single reply on June 27, 2014. *Id.*
11 The *Jewel* Plaintiffs, however, stated that they would agree to the *Shubert* Plaintiffs' request only
12 "if the government [could] assure [them] that no additional data will be destroyed in the
13 meantime." *Id.*

14 In response, the Government Defendants explained that their May 9, 2014 submission
15 addressed their compliance with their preservation obligations, and emphasized that nothing—
16 apart from the *Shubert* Plaintiffs' extension request—had changed since the Court established the
17 briefing schedule regarding this very issue. *Id.* at 3. The *Shubert* Plaintiffs submitted the
18 parties' stipulation seeking additional time on June 2, 2014, *Shubert* ECF No. 122, and, on June
19 3, 2014, this Court granted the requested relief, moving their deadline to June 5, 2014 and the
20 deadline for the Government Defendants' reply to June 27, 2014. ECF No. 234.

21 All the while, the *Jewel* Plaintiffs continued to demand an assurance that "no additional
22 information will be destroyed in the meantime." See Exh. C at 2–3. The Government
23 Defendants reminded Plaintiffs that the Court was aware of the parties' disagreement over the
24 Government's preservation obligations, and that that dispute was already the subject of ongoing
25 briefing. *Id.* 1–2. The Government Defendants offered two proposals to present the issues to the
26 Court within approximately one week, including moving the deadline for their own submission
27 (recently extended by the Court to June 27, 2014 to accommodate the *Shubert* Plaintiffs'
28 extension request) two weeks forward to the original deadline of June 13, 2014. The

1 Government Defendants urged Plaintiffs to avoid emergency briefing on these matters because
2 “[t]he preservation issues at hand are complex and technical, and involve highly significant
3 operational activities of the Intelligence Community under FISC authorization.” *Id.*

4 Plaintiffs refused the Government Defendants’ offers to brief these matters fully by June
5 13, 2014. *Id.* at 1. Instead, Plaintiffs filed an emergency application that identified, for the first
6 time, specific evidence, as opposed to their broad demand that “no additional evidence be
7 destroyed,” *see* Exh C at 1–3. *See* ECF No. 235. In that submission, Plaintiffs referred to
8 “evidence relating to the mass interception of Internet communications [the NSA] is conducting
9 under section 702,” and, in particular, “evidence relating to [the NSA’s] use of ‘splitters’ to
10 conduct bulk interceptions of the content of Internet communications from the Internet
11 ‘backbone’ network of AT&T.” *Id.* at 1. Without supporting citation or explanation, Plaintiffs
12 asserted “[the March 20, 2014 temporary restraining order] and the context in which it was
13 entered” supported a broad interpretation of that order.

14 Before the Government Defendants had the opportunity to explain the complex technical
15 and operational issues implicated by the preservation of material acquired pursuant to Section
16 702—or to be heard as to the likely impact of such an undertaking for the NSA’s national
17 security mission—the Court ordered the Government “not to destroy any documents that may be
18 relevant to the claims at issue in this action, including the Section 702 materials.” Order, *Jewel*
19 ECF No. 236 (June 5, 2014) at 2. Promptly after that order issued, the Government Defendants
20 attempted to contact the Court telephonically, and then moved for an emergency stay of that
21 order, explaining that it “would cause severe operational consequences for the [NSA’a] national
22 security mission.” ECF No. 237.

23 Plaintiffs opposed that emergency motion, asking “How can the *preservation* of these
24 intercepted communications cause a ‘loss of access to lawfully collected signals intelligence
25 information’?” and asserting, without citation or support, “[t]hat information will remain
26 accessible even though it is being preserved.” ECF No. 238 at 1.³ The Declaration of the

27 ³ In the same submission, Plaintiffs argued that the Government should have treated
28 the March 10, 2014 temporary restraining order as extending to activities undertaken pursuant to

1 Deputy Director of the NSA answers Plaintiffs' question, and demonstrates that Plaintiffs'
2 conjectures bear no resemblance to the potentially-affected infrastructure at the NSA or the
3 enormous difficulties and impairment to NSA's core mission that preservation of all Section 702
4 material would entail.

5 ARGUMENT

6 I. PRESERVING ALL SECTION 702 DATA WOULD CREATE SEVERE LEGAL AND 7 TECHNICAL DIFFICULTIES THAT COULD JEOPARDIZE THE OPERATION OF 8 THE PROGRAM AND PLACE NATIONAL SECURITY AT RISK.

9 As set forth in Deputy Director Ledgett's declaration, complying with a mandate to
10 preserve would place the continued operation of the Section 702 program in jeopardy, both in the
11 near and long term.

12 Complying with this Court's June 5 order would significantly undercut critical privacy
13 protections applying to NSA's handling of Section 702 data. Section 702 facilitates the targeted
14 acquisition of foreign intelligence information concerning foreign targets located outside the
15 United States under FISC oversight and in compliance with the Fourth Amendment. *See* 50
16 U.S.C. § 1881a. Under this program, electronic communication service providers supply
17 information to the Government pursuant to authorized directives issued by the Attorney General
18 and the Director of National Intelligence ("DNI"). *See* ODNI Fact Sheet at 1 (June 8, 2013)
19 (attached hereto as Exhibit D); *see* 50 U.S.C. § 1881a(h). The FISA requires the Attorney
20 General and DNI to adopt certain minimization procedures, *see id.* § 1881a(e), the purposes of
21 which are, for example, "to minimize the acquisition and retention, and prohibit the

22 Section 702 "especially in light of the extensive discussions between Court and counsel at the
23 March 19, 2014 hearing on the evidence preservation dispute." ECF No. 238 at 1–2. Plaintiffs
24 cite nothing in the transcript of those proceedings to support their view. *See id.* Indeed, the
25 Court's holdings at the March 19 hearing support the opposite conclusion, since the Court found
26 that the preservation order Plaintiffs proposed for *First Unitarian* was "too broad" and was "not
27 sufficiently tethered to [the] Complaint." Am. Tr. of Proceedings 91:18–24 (Mar. 19, 2014).
28 The Court thus specifically rejected Plaintiffs' contention that the Government should be
required to preserve "telephone records, Internet metadata records, Internet or telephone content
data without regard to when the government obtained them or the legal authority under which the
government obtained them." *See id.* (rejecting Paragraph 1 of Plaintiffs' proposed preservation
order, ECF No. 191-1); *see also supra*, discussing the March 19, 2014 hearing.

1 dissemination, of nonpublicly available information concerning unconsenting United States
2 persons consistent with the need of the United States to obtain, produce, and disseminate foreign
3 intelligence information.” *Id.* §§ 1801(h), 1821(4). The FISC must approve these specific
4 procedures and any amendment to them. *See id.* § 1881a(i).

5 NSA minimization procedures are intended to ensure, *inter alia*, that the collection is
6 consistent with the Fourth Amendment and are too numerous to detail here. *See id.* §
7 1881a(b)(5).⁴ By way of example, though, the NSA must not retain information pursuant to its
8 so-called PRISM collection any longer than “five years from the expiration date of the
9 certification authorizing the collection,” whereas information “known to contain communications
10 of or concerning United States persons [must] be destroyed upon recognition . . .” if it does not
11 meet one of the requirements for retention. *Minimization Procedures Used by the National*
12 *Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant*
13 *to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (“Minimization*
14 *Procedures”)* at 7 (attached hereto as Exhibit E). Similarly, with regard to information acquired
15 through NSA’s “upstream collection techniques,” *id.* at 7,⁵ unevaluated information “may be
16 retained no longer than two years from the expiration date of the certification authorizing the
17 collection,” whereas information that is “known to contain communications of or concerning
18 United States persons will be destroyed upon recognition” if it does not meet one of the
19 requirements for retention. *Id.*⁶ Complying with this Court’s June 5 Order to preserve

21 ⁴ Each agency that receives the Section 702 collection has its own FISC-approved
22 minimization procedures and may retain and disseminate communications acquired under
23 Section 702 only in accordance with those procedures. The Court’s June 5 Order would
24 similarly impact the minimization procedures implemented by the other agencies that receive
25 Section 702-derived information.

26 ⁵ Upstream collection refers to NSA’s collection of telephone and electronic
27 communications as they transit the Internet backbone within the United States.

28 ⁶ The text of this brief refers here only to two examples of retention limits and purging
requirements. Other situations and the associated minimization procedures and compliance
requirements are set forth in detail in the *Minimization Procedures* such as those involving a
change in the target’s location (determined to be inside the United States) or his status
(determined to be a U.S. person), attorney-client communications, “domestic communications,”
and “foreign communications of or concerning United States persons.” *Minimization Procedures*

1 indefinitely all Section 702 material will conflict with these current time limits for the retention
 2 of data as well as the requirements that certain information be destroyed “upon recognition.” *See*
 3 *Minimization Procedures* at 7-9.

4 Amending the current minimization procedures—which is no small matter and cannot be
 5 done immediately to comply with this Court’s June 5 Order⁷—to appropriately adjust all the
 6 retention limits and all purging requirements will place the program in jeopardy. *See* Ledgett
 7 Decl. ¶ 2 (declaring that NSA cannot effectuate this Court’s order while remaining in compliance
 8 with the statute and related FISC orders). The FISC has previously approved the NSA’s
 9 minimization procedures for collections under Section 702. *See* Aug. 24, 2012 FISC Op., 2012
 10 WL 9189263, at *2-3; Nov. 30, 2011 FISC Op., 2011 WL 10947772; Oct. 3, 2011 FISC Op.,
 11 2011 WL 10945618. To take one example, however, in an opinion issued on October 3, 2011,
 12 the FISC found that the NSA’s minimization procedures as applied to one aspect of the proposed
 13 collection—NSA’s upstream collection of internet transactions containing multiple
 14 communications, or “MCTs”—was statutorily and constitutionally deficient. *See* Oct. 3, 2011
 15 FISC Op., 2011 WL 10945618.⁸

16
 17 at 7-9. All of these procedures will be impacted if the NSA were to comply with the Court’s
 18 June 5 Order.

19 ⁷ The Attorney General and the Director of National Intelligence (“DNI”), who are
 20 responsible for amending the statutorily-based minimization procedures, *see* 50 U.S.C. §
 21 1881a(i)(1)(C), must execute under oath an amended certification that contains the requisite
 22 statutory findings concerning the amended minimization procedures, that is, the certification
 23 must contain the findings that the amended procedures meet the statutory definition of
 24 minimization procedures, will be submitted to the FISC for approval, and are *consistent with the*
 25 *requirements of the Fourth Amendment*. *See id.* §§ 1881a(g)(1)(A), (2)(A)(ii) & (iv). Pursuant
 26 to the FISA, the FISC then has 30 days in which to review the amended certification and
 27 minimization procedures and to issue an order either approving them or finding them deficient.
 28 *See id.* § 1881a(i)(1)(B) & (3)(A), (B). Although the Attorney General and DNI can authorize
 the use of the amended minimization procedures pending the FISC’s review, so that the
 amendment could be effective immediately upon execution, *see* 50 U.S.C. § 1881(a)(i)(1)(C), the
 FISC would still have to approve the certification and minimization procedures. At bottom, even
 if NSA could otherwise comply with this Court’s June 5 order, compliance could not begin
 immediately.

⁸ The Deputy Director of the NSA provides another example. If the NSA was prohibited
 from purging inadvertently acquired communications of American citizens and other U.S.

1 In that opinion, the FISC explained that, under the NSA's then-proposed minimization
2 procedures, thousands of wholly domestic communications and other discrete communications
3 that are not to or from a targeted selector but that are to, from, or concerning a United States
4 person could be retained by the NSA for at least five years, even if the communications had no
5 direct connection to a targeted selector and thus were unlikely to contain foreign intelligence
6 information. *See id.* at * 17-29. As a result, the FISC concluded that the proposed NSA
7 minimization procedures failed to meet the statutory requirements of minimization procedures
8 and did not pass constitutional muster. *Id.* The Attorney General and DNI adopted new
9 minimization procedures designed to cure these deficiencies and sought the FISC's approval as
10 required. *See* Nov. 30, 2011 FISC Mem. Op., *available at*
11 [http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa)
12 [declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa)
13 [foreign-intelligence-surveillance-act-fisa.](http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa)

14 The FISC's rationale for approving these new procedures as compliant with FISA and
15 consistent with the requirements of the Fourth Amendment is instructive here. *See id.* at 11-15.
16 As for the then-newly proposed two-year retention limits for upstream acquisitions, the FISC
17 found that this limit "strikes a more reasonable balance between the government's national
18 security needs and the requirements that non-target information concerning United States
19 persons and persons in the United States be protected." *Id.* at 13. The "principal problem," the
20 FISC continued, with the measures previously proposed that the FISC had rejected was that
21 "rather than requiring the identification and segregation of information 'not relevant to the
22 authorized purpose of the acquisition' or the destruction of such information promptly following
23 acquisition, NSA's [previously proposed] handling of MCTs *tended to promote the retention of*
24 *information*, including information of or concerning United States persons with no direct
25 connection to any target." *Id.* at 14 (emphasis added).

26
27
28 persons as this Court's order of June 5 seems to require, such a situation could create a violation
of a statute, 50 U.S.C. § 1809, which contains criminal penalties. Ledgett Decl. ¶ 4.

1 So too here. The Court’s June 5 Order *requires* the retention of this type of information
2 indefinitely that might be otherwise purged upon recognition or aged-off after the pertinent time
3 period. By requiring that information be retained indefinitely, the Court’s order destroys “the
4 reasonable balance” the FISC found to have satisfied statutory and Constitutional requirements
5 for upstream collection. *See* FISC Mem. Op. (Nov. 30, 2011), at 13. These are but two
6 examples. The Court’s June 5 Order cannot be reconciled with the FISC-approved procedures
7 that have been carefully designed to be consistent with the Constitution and with the “need of the
8 United States to obtain, produce, and disseminate foreign intelligence information.” 50 U.S.C. §
9 1801(h).

10 In addition to putting the Section 702 program in jeopardy, compliance with this Court’s
11 order of June 5 is also likely to have “an immediate, specific, and harmful impact on the national
12 security of the United States” because the NSA may not be able to comply immediately with the
13 order without shutting down the Section 702 program. *See* Ledgett Decl. ¶ 2. The impact of
14 compliance with this Court’s June 5 Order on the NSA—and on the national security of this
15 country—would have immediate adverse consequences. In the near term, attempts to fully
16 comply with the Court’s June 5 Order would be a massive and uncertain endeavor because the
17 NSA may have to shut down all databases and systems that contain Section 702 information in
18 an effort to comply. *See id.* ¶¶ 2-3.

19 The reason why the NSA would have to suspend these operations is that the NSA’s
20 databases are optimized to ensure compliance with the legal requirements of FISA, which
21 includes the FISC-authorized and approved minimization procedures for the retention of
22 information as well as the NSA’s legal obligation to purge or otherwise promptly destroy certain
23 information it collects, as discussed above. *See id.* ¶ 3. And, unlike bulk telephony metadata
24 collected under the Section 215 program, communications acquired pursuant to Section 702
25 resides within multiple databases contained on multiple, operationally complex systems. *See id.*
26 ¶ 3. This means that, as an initial step in attempting to comply with this Court order, the NSA
27 may need to take all databases containing Section 702 data offline while NSA operators and
28 technical staff determine whether and how all of the data that would otherwise be destroyed in

1 order to comply with the FISA and the Constitution could be retained indefinitely instead in
2 compliance with this Court's June 5 Order. *See id.* ¶ 5. Prior to implementing these changes,
3 the NSA must thoroughly develop and test the proposed modifications in order to avoid
4 unforeseen consequences that could cause FISC compliance problems or impact the NSA's
5 ability to provide foreign intelligence to protect the country. *See id.*

6 Throughout this period of time, NSA analysts would be unable to access foreign
7 intelligence information already stored in these repositories, and the NSA would be unable to
8 ingest (or add) any incoming foreign intelligence information into these repositories for review
9 and analysis. *See id.* This direct loss of access to significant foreign intelligence would
10 immediately impact the national security of the United States. *Id.* ¶ 3. As numerous officials
11 within the Intelligence Community have publicly stated, and as the evidence shows, the
12 acquisition of communications pursuant to Section 702 of the FISA is the most significant tool in
13 the NSA's collection arsenal for the detection, identification, and disruption of terrorist threats to
14 the U.S. and around the world. *Id.* ¶ 7. For example, the information gathered under this
15 program has provided the U.S. Government with "critical leads to help prevent potential terrorist
16 events in countries around the world, has yielded intelligence regarding proliferation networks,
17 has directly and significantly contributed to successful operations to impede the proliferations of
18 weapons of mass destruction and related technologies, and has provided significant and unique
19 intelligence regarding potential cyber threats. *Id.*

20 In short, as the Deputy Director of the NSA concluded, any decision that might impair
21 NSA operations in this manner could immediately deprive the nation of this valuable tool and
22 cause immediate and grave danger to the national security. *Id.*⁹

24 ⁹ The Deputy Director of the NSA also notes that, in the short and long-term, an order
25 prohibiting the destruction of any Section 702 data will cause a lack of or delay of access to
26 lawfully collected signals intelligence because (1) the NSA has only a finite amount of data
27 storage capacity and so the NSA would be limited in its ability to store newly collected non-
28 Section 702 data; (2) implementation of the Court's order would introduce latency into the
system (such as lengthening the query response time for analysts) which could prevent analysts
from identifying, analyzing, and disseminating critical intelligence to prevent an attack; and (3)
there will be foreseen and unforeseen consequences to implementing the Court's June 5 Order,

1 II. THE COURT’S TEMPORARY RESTRAINING ORDER DOES NOT INCLUDE
 2 SECTION 702 MATERIALS, NOR ARE SECTION 702 MATERIALS RELEVANT
 3 TO PLAINTIFFS’ CLAIMS.

4 The TRO that Plaintiffs seek to enforce does not apply to Section 702 materials, either
 5 expressly or implicitly.¹⁰ See Fed. R. Civ. P. 65(d)(1) (“Every order granting an injunction and
 6 every restraining order must . . . state its terms specifically; and describe in reasonable detail . . .
 7 the act or acts restrained or required.”); see also *Del Webb Cmty., Inc. v. Partington*, 652 F.3d
 8 1145, 1150 (9th Cir. 2011). Plaintiffs never sought a temporary restraining order over these
 9 materials—a fact made clear in their original motion for a temporary restraining order. That
 10 motion did not request relief regarding Section 702 activities, but rather, concerned “the same
 11 telephonic records at issue in *First Unitarian Church v. NSA*,” which Plaintiffs repeatedly
 12 specified as bulk “telephone metadata records” or “call-detail records.” Pls.’ Ex Parte Mot. for
 13 TRO, Dkt. No. 186 at 1, 2; see *id.* at 3-4 (“The *Jewel* complaint alleged unlawful and
 14 unconstitutional acquisition of call-detail records, including the ‘call-detail records collected
 15 under the [NSA’s] bulk telephony metadata program While the Plaintiff[s] ultimately want
 16 the call-detail records destroyed at the conclusion of the case, there is no doubt that the call-
 17 records ‘may be relevant’ in the interim.”); see also Pls.’ Ex Parte Mot. for TRO in *First*

18 which could include scheduled and unscheduled outages to ensure FISC compliance and
 19 compliance with this Court’s order. See Ledge Decl. ¶ 8.

20 ¹⁰ If the Court were to construe Plaintiffs’ application as a motion for a new TRO to
 21 cover Section 702 materials, such a motion should be denied not only for the reasons that follow,
 22 but also for failure to establish any of the requirements for an “extraordinary and drastic remedy”
 23 before the merits of the preservation dispute have been decided. *Munaf v. Geren*, 553 U.S. 674,
 24 689-90 (2008); see also *Stuhlberg Int’l Sales Co., Inc. v. John D. Brush & Co.*, 240 F.3d 832,
 25 839 n.7 (9th Cir. 2001) (standard for a TRO is the same as for a preliminary injunction). Such
 26 drastic relief is appropriate only “upon a clear showing that the plaintiff is entitled to such
 27 relief,” including the demonstration “(1) that it is likely to succeed on the merits, (2) that it is
 28 likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of
 equities tips in its favor, and (4) that an injunction is in the public interest.” *Earth Island Inst. v.*
Carlton, 626 F.3d 462, 469 (9th Cir. 2010) (citing *Winter v. NRDC*, 555 U.S. 7, 19 (2008)).
 Plaintiffs bear the burden of demonstrating that each of these four factors is met. *DISH Network*
Corp. v. FCC, 653 F.3d 771, 777 (9th Cir. 2011). “[A]n injunction must be narrowly tailored . . .
 to remedy only the specific harms shown by the plaintiffs rather than to enjoin all possible
 breaches of the law.” *Iconix, Inc. v. Tokuda*, 457 F. Supp. 2d 969, 998 (N.D. Cal. 2006) (citing
Price v. City of Stockton, 390 F.3d 1105, 1117 (9th Cir. 2004)).

1 *Unitarian*, 08-cv-3287, Dkt. No. 86 (same in every respect). Nor have Plaintiffs at any time
2 sought to extend the scope of the TRO beyond the bulk collection of telephony metadata. *See*,
3 *e.g.*, Am. Tr. of Proceedings at 62:5–9 (Counsel for Plaintiffs) (“[W]e specifically excluded from
4 the class in *Jewel* anybody who was involved with a terrorist [organization]. We’re talking about
5 ordinary people and bulk collection.”), *and id.* at 62:25– 63:5 (“[T]he idea here is to map the
6 preservation obligations to the allegations of the Complaint. And the allegations of the
7 Complaint are about bulk collection”). Because “an injunction should be tailored to eliminate
8 *only the specific harm alleged*,” *Experience Hendrix L.L.C. v. Hendrixlicensing.com, LLC*, 742
9 F.3d 377, 388 (9th Cir 2014) (internal quotation omitted), it would be error to interpret the TRO
10 beyond its terms and the harms alleged in Plaintiffs’ original motion.

11 The context surrounding Plaintiffs’ original motion for a temporary restraining order
12 likewise underscores its specific focus. That motion, and the TRO resulting therefrom, dealt
13 with the specific context of the impending destruction of aged-off bulk telephony metadata
14 obtained pursuant to Section 215 of the FISA, in compliance with FISC-ordered data retention
15 limits. *See* Gov’t Defs.’ Notice Regarding Order of the FISC (filed in *First Unitarian*, No. 13-
16 cv-3287, Dkt. No. 85) (notifying Court and Plaintiffs of the FISC’s denial of the Government’s
17 motion for leave to retain call-detail records beyond FISC-ordered retention deadlines). *See also*
18 *supra* at 3-5.

19 In the face of the language of the TRO, the motion that precipitated it, the statements
20 made by Plaintiffs’ counsel in open court, and the context surrounding the parties’ preservation
21 dispute, Plaintiffs would nevertheless have this Court believe that its TRO related to bulk
22 telephony metadata covers the “destruct[ion of] evidence relating to surveillance under section
23 702,” *see* Pls. Mot., Ex. E. But not only did Plaintiffs not seek a temporary restraining order
24 over such materials, *see supra*, they did not even raise the potential preservation of Internet or
25 telephone content generally (not Section 702 materials specifically) until *after* the TRO was
26 entered and *after* being told by this Court that the occasion for its issuance was the impending
27 destruction of aged-off bulk telephony metadata, during later briefing. *See* Pls.’ Opening Br. Re
28 Evid. Preservation at 1 (ECF No. No. 191). That later briefing led to a preservation order in the

1 *First Unitarian* case—an order that concerns the bulk telephony metadata program, not Section
2 702 activities—and to the Court establishing a separate briefing schedule to resolve the parties’
3 disagreement regarding the scope of the Government’s preservation obligations in *Jewel* and
4 *Shubert*. See Am. Minute Order, Dkt. No. 206 at 2.

5 In sum, the TRO Plaintiffs seek to enforce was intended to prevent, and does prevent, the
6 destruction of Section 215 telephony metadata that was scheduled to age-off pursuant to
7 retention limitations imposed by the FISC as a condition for its collection. It does not apply to
8 Section 702 materials, nor did the context in which it was entered involve such materials.

9 The burden to the Government and harm to the NSA’s mission from preserving all
10 Section 702 material is particularly unwarranted given the irrelevance of this material to
11 Plaintiffs’ claims. As the Court is aware, the Government vigorously disputes that Plaintiffs’
12 claims encompass any FISC-authorized activity, given, among other things, the fact that the
13 complaints challenge intelligence-gathering activities that occurred without any statutory or
14 judicial authority. However, to read those complaints as challenging activity authorized by
15 Section 702 would be particularly egregious. Section 702 is a publicly acknowledged
16 intelligence collection program that clearly operates pursuant to both statutory and judicial
17 authority. It was enacted before Plaintiffs filed their complaint, and was challenged in a public
18 lawsuit the day it was enacted in 2008. See *Clapper v. Amnesty International*, 133 S. Ct. 1138,
19 1146 (2013). Plaintiffs did not, however, challenge any Section 702 activities in their complaint,
20 and they subsequently disavowed any relevance of Section 702 to their claims. See Gvt. Defs.’
21 Brief Regarding Compliance with Preservation Orders at 16-17 (ECF No. 229).

22 Moreover, the common thread of Plaintiffs’ claims is a challenge to mass surveillance
23 activities—i.e., the bulk, “dragnet” collection of communications and communications records—
24 in contrast to targeted surveillance activities. Section 702 undisputedly permits the targeting of
25 non-U.S. persons reasonably believed to be located outside the United States in order to acquire
26 foreign intelligence information. Section 702 does not authorize the bulk acquisition of domestic
27 communications, nor does it permit the targeting of any person known to be in the United States
28 or any U.S. person reasonably believed to be located abroad. See 50 U.S.C. §§ 1881a(a), (b);

1 *Clapper v. Amnesty International*, 133 S. Ct. 1138, 1144 (2013); *Klayman v. Obama*, 957 F.
2 Supp. 2d 1, 8 n.6 (D.D.C. 2013).

3 Plaintiffs themselves emphasized this distinction, with respect to Section 702, as recently
4 as January of this year. In explaining why footnote four of *Amnesty International* does not apply
5 to their case,¹¹ Plaintiffs told the Court that deciding their “claims of *untargeted* surveillance will
6 not reveal who the government has targeted for surveillance, because that fact is irrelevant and
7 unnecessary to plaintiffs’ claims.” Plaintiffs’ Responses to the Court’s Four Questions at 10
8 (ECF No. 177). They went on to distinguish claims based on Section 702 from their case as
9 follows:

10 *Clapper* was a targeted surveillance lawsuit, not an untargeted surveillance
11 lawsuit like this one. . . . The *Clapper* plaintiffs made a facial challenge to the
12 constitutionality of 50 U.S.C. § 1881a (section 702 of FISA), a statute that
13 authorizes only targeted surveillance **The *Clapper* plaintiffs alleged their
14 future communications likely would be intercepted because they
15 communicated with persons who were likely targets of surveillance, not
16 because they were subject to a program of untargeted mass surveillance.**

17 *Id.* at 10-11 (emphasis added). Plaintiffs cannot have it both ways—they cannot maintain one
18 view of the scope of their claims for purposes of arguing that the Government is destroying
19 potentially relevant evidence, and the opposite view for purposes of arguing that *Amnesty*
20 *International*’s footnote four does not apply to their case.

21 Consistent with these statements, Plaintiffs have not alleged that they were targeted under
22 Section 702 (which would be implausible since Plaintiffs are U.S. persons), or that they
23 communicated or communicate with anyone who was or is targeted under Section 702. To the
24 extent that Plaintiffs will argue that the Section 702 program is a program of untargeted mass
25 surveillance based on the fact that, due to technological limitations, NSA’s upstream collection
26 results in the acquisition of Internet transactions containing multiple communications, it is purely
27 speculative that Plaintiffs’ communications are included in this incidental overcollection. In

28 ¹¹ See *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1113 (N.D. Cal. 2013) (explaining that
footnote four of *Amnesty International* “not[es] that, pursuant to hypothetical *in camera*
proceedings permitted under [50 U.S.C.] § 1806(f), ‘the court’s postdisclosure decision about
whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his
name was on the list of surveillance targets.’”).

1 2011, NSA's upstream collection constituted only approximately 9% of the total Internet
2 communications being acquired by the NSA under Section 702. Oct. 3, 2011 FISC opinion,
3 2011 WL 10945618, at * 9.

4 An argument based on incidental overcollection under upstream also overlooks the fact
5 that the NSA has implemented a host of minimization procedures, which the FISC has approved,
6 pursuant to which the NSA, *inter alia*, (1) identifies and segregates those types of Internet
7 transactions that are most likely to contain wholly domestic communications and non-target
8 communications to or from U.S. persons or persons located in the United States, (2) restricts
9 analysts' access to segregated transactions, (3) destroys transactions determined to contain
10 wholly domestic communications, and (4) destroys all Internet transactions two years after the
11 date of the certification authorizing the collection. *See* November 30, 2011 FISC opinion at 7-
12 15. Thus, even if Plaintiffs' communications had in fact been incidentally acquired under NSA's
13 upstream collection (a highly speculative proposition), the minimization procedures make it
14 "exceedingly unlikely" that any of those communications have been maintained. Ledgett Decl. ¶
15 9. An order requiring the preservation of all Section 702 material would, ironically, abrogate the
16 very protections put in place by the FISC to ensure that the NSA's upstream collection complies
17 with the Fourth Amendment, all so that Plaintiffs can attempt to show that it did not.

18 CONCLUSION

19 For all the foregoing reasons, the Court should deny Plaintiffs' Emergency Application to
20 Enforce the Court's Temporary Restraining Order and vacate its June 5, 2014 order.

21 Dated: June 6, 2014

Respectfully Submitted,

22 STUART F. DELERY
23 Assistant Attorney General

24 JOSEPH H. HUNT
25 Director, Federal Programs Branch

26 /s Anthony J. Coppolino
27 ANTHONY J. COPPOLINO
28 Deputy Branch Director

1 JAMES J. GILLIGAN
2 Special Litigation Counsel
james.gilligan@usdoj.gov

3 */s/ Marcia Berman*
4 MARCIA BERMAN
5 Senior Trial Counsel
marcia.berman@usdoj.gov

6 BRYAN DEARINGER
7 RODNEY PATTON
8 JULIA BERMAN
9 Trial Attorneys

10 U.S. Department of Justice
11 Civil Division, Federal Programs Branch
12 20 Massachusetts Avenue, NW, Rm. 6102
13 Washington, D.C. 20001
14 Phone: (202) 514-4782
15 Fax: (202) 616-8460

16 *Attorneys for the Government Defendants*