STUART F. DELERY
Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
BRYAN DEARINGER
Trial Attorney
RODNEY PATTON
Trial Attorney
JULIA BERMAN
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 7346
Washington, D.C. 20001
Phone: (202) 514-4782; Fax: (202) 616-8470

Attorneys for the Government Defendants in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, 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

INTRODUCTION

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

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

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

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

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

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

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

BACKGROUND

The March 10, 2014 Temporary Restraining Order

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

Citing the Government's filing before the FISC, Plaintiffs emailed the Government Defendants seeking "specific reaffirmation that bulk telephone records collected by the NSA have been preserved in the Jewel case." ECF No. 186, Exh. E at 7. Plaintiffs then sought a temporary restraining order "prohibiting . . . [the Government Defendants] from destroying any evidence relevant to the claims at issue in this action, including but not limited to prohibiting the destruction of any telephony metadata or 'call detail' records." *Id.* at 1.[2] On March 10, 2014,

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

[2] Although Plaintiffs' motion for a temporary restraining order claimed that "[t]here has been litigation challenging the lawfulness of the government's telephone metadata collection activity, Internet metadata collection activity, and upstream collection activity pending in the Northern District of California continuously since 2006," ECF No. 186 at 2, Plaintiffs provide no 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).

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

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

At the same hearing, the Court rejected Plaintiffs' request that the Government Defendants, within 15 days, "disclose whether they have destroyed telephone records, Internet metadata records, Internet or telephone content data, or any other evidence potentially relevant to these lawsuits since the commencement of *Hepting, et al. v. AT&T et al.* litigation (No. 06-cv-0672) in January 2006." *See id.* at 91:16–17 (rejecting Paragraph 4 of Plaintiffs' proposed preservation order, ECF No. 191-1). Indeed, the Court specifically refused to order preservation of "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.* at 91:18–24 (rejecting Paragraph 1 of Plaintiffs' proposed preservation order, ECF No. 191-1), because this requirement was "too broad" and "the Plaintiffs' suggested language on the scope of materials to be preserved [was] not sufficiently tethered to their Complaint." *Id.* at 91: 18–19, 22–24. The Court then specifically directed, in the context of addressing the preservation order for *First Unitarian*, that preservation obligations should extend no farther than "the evidence that relates to the precise claims made by Plaintiffs in [their] complaint." *Id.* at 91:24–92:2.

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

The Current Dispute

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

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

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

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

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

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

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

Plaintiffs opposed that emergency motion, asking "How can the *preservation* of these intercepted communications cause a 'loss of access to lawfully collected signals intelligence information'?" and asserting, without citation or support, "[t]hat information will remain accessible even though it is being preserved." ECF No. 238 at 1.[3] The Declaration of the

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

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

ARGUMENT

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

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

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

---

Section 702 "especially in light of the extensive discussions between Court and counsel at the March 19, 2014 hearing on the evidence preservation dispute." ECF No. 238 at 1–2. Plaintiffs cite nothing in the transcript of those proceedings to support their view. *See id.* Indeed, the Court's holdings at the March 19 hearing support the opposite conclusion, since the Court found that the preservation order Plaintiffs proposed for *First Unitarian* was "too broad" and was "not sufficiently tethered to [the] Complaint." Am. Tr. of Proceedings 91:18–24 (Mar. 19, 2014). 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.

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

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

---

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

[5] Upstream collection refers to NSA's collection of telephone and electronic communications as they transit the Internet backbone within the United States.

[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

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

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

---

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

[7] The Attorney General and the Director of National Intelligence ("DNI"), who are responsible for amending the statutorily-based minimization procedures, *see* 50 U.S.C. § 1881a(i)(1)(C), must execute under oath an amended certification that contains the requisite statutory findings concerning the amended minimization procedures, that is, the certification must contain the findings that the amended procedures meet the statutory definition of minimization procedures, will be submitted to the FISC for approval, and are *consistent with the requirements of the Fourth Amendment*. *See id.* §§ 1881a(g)(1)(A), (2)(A)(ii) & (iv). Pursuant to the FISA, the FISC then has 30 days in which to review the amended certification and minimization procedures and to issue an order either approving them or finding them deficient. *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.

In that opinion, the FISC explained that, under the NSA's then-proposed minimization procedures, thousands of wholly domestic communications and other discrete communications that are not to or from a targeted selector but that are to, from, or concerning a United States person could be retained by the NSA for at least five years, even if the communications had no direct connection to a targeted selector and thus were unlikely to contain foreign intelligence information. *See id.* at * 17-29. As a result, the FISC concluded that the proposed NSA minimization procedures failed to meet the statutory requirements of minimization procedures and did not pass constitutional muster. *Id.* The Attorney General and DNI adopted new minimization procedures designed to cure these deficiencies and sought the FISC's approval as required. *See* Nov. 30, 2011 FISC Mem. Op., *available at* 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.

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

---

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.

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

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

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

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

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

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

[9] The Deputy Director of the NSA also notes that, in the short and long-term, an order prohibiting the destruction of any Section 702 data will cause a lack of or delay of access to lawfully collected signals intelligence because (1) the NSA has only a finite amount of data storage capacity and so the NSA would be limited in its ability to store newly collected non-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,

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

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

---

which could include scheduled and unscheduled outages to ensure FISC compliance and compliance with this Court's order. *See* Ledgett Decl. ¶ 8.

[10] If the Court were to construe Plaintiffs' application as a motion for a new TRO to cover Section 702 materials, such a motion should be denied not only for the reasons that follow, but also for failure to establish any of the requirements for an "extraordinary and drastic remedy" before the merits of the preservation dispute have been decided. *Munaf v. Geren*, 553 U.S. 674, 689-90 (2008); *see also Stuhlbarg Int'l Sales Co., Inc. v. John D. Brush & Co.*, 240 F.3d 832, 839 n.7 (9th Cir. 2001) (standard for a TRO is the same as for a preliminary injunction). Such drastic relief is appropriate only "upon a clear showing that the plaintiff is entitled to such relief," including the demonstration "(1) that it is likely to succeed on the merits, (2) that it is 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)).

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

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

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

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

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

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

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

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

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

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

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

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

---

[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.'").

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

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

CONCLUSION

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

Dated: June 6, 2014

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

/s Anthony J. Coppolino
ANTHONY J. COPPOLINO
Deputy Branch Director

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

/s Marcia Berman
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov

BRYAN DEARINGER
RODNEY PATTON
JULIA BERMAN
Trial Attorneys

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

Attorneys for the Government Defendants