CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Counsel

JULIA A. BERMAN
CAROLINE J. ANDERSON
TIMOTHY A. JOHNSON
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 7320
Washington, D.C. 20001
E-mail: rodney.patton@usdoj.gov
Phone: (202) 305-7919
Fax: (202) 616-8470

Attorneys for the Government Defendants
Sued in their Official Capacities

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-04373-JSW **GOVERNMENT DEFENDANTS' OPENING BRIEF REGARDING PRESERVATION OF UPSTREAM INTERNET COMMUNICATIONS PREVIOUSLY ACQUIRED UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT** Hon. Jeffrey S. White

TABLE OF CONTENTS

PAGE

INTRODUCTION 1

BACKGROUND 3

Prior Proceedings Concerning Preservation Issues 3

FISA Section 702 4

Upstream Collection of MCTs 6

Recent FISC-Approved Changes to Upstream Collection and Mandatory Destruction of Previously Acquired Transactions 8

Relevant Proceedings in this Court 9

ARGUMENT 11

I. LITIGANTS' DUTY TO MAKE PRESERVATION EFFORTS THAT ARE REASONABLE AND PROPORTIONAL TO THE NEEDS OF THE CASE 11

II. THE GOVERNMENT'S PROPOSAL FOR TARGETED PRESERVATION OF LEGACY UPSTREAM COMMUNICATIONS THAT ARE TO OR FROM THE PLAINTIFFS (IF ANY) CONSTITUTES A REASONABLE AND PROPORTIONAL APPROACH TO THE PRESERVATION OF POTENTIALLY RELEVANT EVIDENCE 13

III. WHOLESALE PRESERVATION OF LEGACY UPSTREAM DATA WOULD UNNECESSARILY CONTRAVENE EFFORTS BY THE NSA AND THE FISC TO PROTECT IMPORTANT FOURTH AMENDMENT INTERESTS AND WOULD BE NEITHER REASONABLE NOR PROPORTIONAL 16

CONCLUSION 17

TABLE OF AUTHORITIES

CASES **PAGE(S)**

Apple Inc. v. Samsung Elec. Co., Ltd.,
881 F. Supp. 2d 1132 (N.D. Cal. 2012) 11

In re Broiler Chicken Antitrust Litig.,
2017 WL 1682572 (N.D. Ill. Apr. 21, 2017) 13

City of Wyoming v. Procter & Gamble Co.,
2016 WL 6908110 (D. Minn. Oct. 7, 2016) 13

Clapper v. Amnesty Int'l, USA,
133 S. Ct. 1138 (2013) 5

FTC v. DirecTV, Inc.,
2016 WL 7386133 (N.D. Cal. Dec. 21, 2016) 13

Martinelli v. Johnson & Johnson,
2016 WL 1458109 (E.D. Cal. Apr. 13, 2016) 13

In re Napster, Inc. Copyright Litig.,
462 F. Supp. 2d 1060 (N.D. Cal. 2006) 11

Little Hocking Water Assn., Inc. v. E.I. du Pont de Nemours & Co.,
94 F. Supp. 3d 893 (S.D. Ohio 2015) 11-12

Pippins v. KPMG LLP,
279 F.R.D. 245 (S.D.N.Y. 2012) 12

[*Redacted Caption*],
2011 WL 10945618 (F.I.S.C. Oct. 3, 2011) 6, 7, 16

[*Redacted Caption*],
2011 WL 10947772 (F.I.S.C. Nov. 30, 2011) 7, 8

[*Redacted Caption*],
2012 WL 9189263 (F.I.S.C. Aug. 24, 2012) 8

Rimkus Consulting Grp., Inc. v. Cammarata,
688 F. Supp. 2d 598 (S.D. Tex. 2010) 11

Rogers v. Averitt Express, Inc.,
215 F. Supp. 3d 510 (M.D. La. 2017) 11

Silvestri v. Gen. Motors Corp.,
271 F.3d 583 (4th Cir. 2001) 11

Starline Windows Inc. v. Quanex Bldg. Prod. Corp.,
2016 WL 4485568 (S.D. Cal. Aug. 19, 2016) 11, 15, 17

Victor Stanley, Inc. v. Creative Pipe, Inc.,
269 F.R.D. 497 (D. Md. 2010) 11

Zbylski v. Douglas Cty. Sch. Dist.,
154 F. Supp. 3d 1146 (D. Colo. 2015) 11

STATUTES

50 U.S.C. § 1881a 5-6
FISA Amendments Act of 2008,
Pub. L. No. 110-261 (2008), 121 Stat. 522 5

FEDERAL RULES OF CIVIL PROCEDURE

Fed. R. Civ. P. 26 ..... 11, 12, 13
Fed. R. Civ. P. 34 11
Fed. R. Civ. P. 26 Advisory Comm. Notes to 2015 Amendments 12
Fed. R. Civ. P. 37(e) Advisory Comm. Notes to 2015 Amendments 12

MISCELLANEOUS

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) 6

U.S. District Court for the Northern District of California,
Guidelines for the Discovery of Electronically Stored Information 8

INTRODUCTION

The preservation issue now before the Court concerns electronic communications data acquired by defendant National Security Agency ("NSA"), using its "Upstream" Internet acquisition technique, prior to changes in the manner in which Upstream Internet acquisition is conducted that were recently approved by the Foreign Intelligence Surveillance Court ("FISC"). These "legacy" Upstream Internet communications data contain communications that have been of special statutory and constitutional concern to the FISC, and their preservation implicates significant Fourth Amendment interests. Under the recent changes to Upstream Internet acquisition, the NSA is now obligated by FISC-approved minimization procedures—with which Section 702 of Foreign Intelligence Surveillance Act ("FISA") requires the NSA to comply—to destroy the legacy Upstream Internet communications data "as soon as practicable."

In 2014 this Court denied Plaintiffs' request for an order requiring the Government to preserve all "Section 702" materials, including raw Upstream Internet communications data acquired by the NSA. Notwithstanding that the Government thus has no current obligation in this case to preserve the legacy Upstream Internet communications data, it has not yet commenced the accelerated age off of the aforementioned data contained in its central repository pending this Court's resolution of any objection by Plaintiffs to their accelerated destruction. Since the May 19, 2017, case management conference the parties have communicated several times about this issue, but have not yet succeeded in resolving their differences. The Government therefore submits this memorandum to propose the following resolution of the parties' dispute.

Specifically, the Government Defendants propose that the Court order:

- That the *Jewel* and *Shubert* Plaintiffs provide to the Government the e-mail addresses that they have used since 2014 (an outer bound on the date range of the legacy Upstream Internet communications data), and the dates during which they used those addresses;

- That the NSA take those steps necessary to identify and preserve any Upstream Internet communications data to or from the e-mail addresses identified by Plaintiffs, if any such communications containing those e-mail addresses exist in the legacy Upstream Internet communications data contained in the NSA's central repository;

- That the NSA sequester any Upstream Internet communications of Plaintiffs identified through the process described above for the pendency of the respective actions, such that neither the NSA nor any other agency would have analytic access to those communications, with only technical access permitted for purposes of maintaining data integrity and such other access as may be needed for purposes of this litigation;

- That, because the identification of Plaintiffs' communications contained in the legacy Upstream Internet communications data, if any, would involve access to that information arguably in contravention of NSA's FISC-approved Section 702 minimization procedures, the Government first notify the FISC of the Court's order, and notify this Court of any objections raised by the FISC, before proceeding as described;

- That nothing in the Court's order itself is to be construed as requiring the Government to inform Plaintiffs, or otherwise publicly state, whether or not any of Plaintiffs' communications were located in the legacy Upstream Internet communications data, the existence or non-existence of such communications being a classified fact; and

- That the Government Defendants, upon completion of the identification described above and the sequestration, as described above, of any communications of Plaintiffs identified as a result, will be under no obligation to preserve any other legacy Upstream Internet communications data for purposes of the *Jewel* and *Shubert* cases.

The process described above is a reasonable and proportional approach to preserving information potentially relevant to Plaintiffs' standing because e-mails are an unclassified (and thus workable) example of a selector that could be used to identify specific communications involving Plaintiffs.

The alternative to such a targeted preservation approach is one that requires the Government to preserve all of the legacy Upstream Internet communications data on the theory that somewhere in that set of communications there could be evidence of Plaintiffs' standing. Such an approach, however, implicates the privacy interests of other U.S. persons who are not parties to this litigation by requiring the Government to retain indefinitely non-relevant U.S. persons' communications. Protection of these privacy interests is precisely why the FISC has slated those communications for destruction.

And it is precisely this concern that is animating the Government's request that the Court resolve this preservation dispute without delay. To that end, the Government

Defendants request that the Court enter this relief not only in *Jewel* but also, to avoid undue delay, in the companion case of *Shubert v. Trump*, 07-cv-693.[1]

BACKGROUND

Prior Proceedings Concerning Preservation Issues

On November 16, 2009, the Court entered an evidence-preservation order reminding the parties of their obligation to preserve evidence that may be relevant to this action, and directing them to halt the routine destruction of relevant materials, to the extent practicable, for the pendency of the case. *See* ECF No. 51, ¶¶ A, D.

In 2014, disputes arose between the parties regarding the scope of the Government's preservation obligations under the Court's order and whether the Government Defendants had complied with those obligations. The first dispute arose in March 2014 when the Government, citing its common-law preservation obligations in pending civil litigation, moved for relief from the FISC from the requirement that bulk telephony metadata acquired under Section 215 of the USA Patriot Act be destroyed within five years of acquisition. The FISC initially denied the request. Thereafter, the Government filed public notices in cases that challenged the legality of the NSA's Section 215 bulk telephony metadata program, which stated that, absent court order to the contrary, the Government had to begin destroying metadata acquired more than five years prior. *See, e.g.*, *Klayman v. Obama*, 13-cv-0851 (D.D.C.), ECF No. 94.

Plaintiffs in this case sought and obtained a temporary restraining order ("TRO") prohibiting such destruction of bulk telephony metadata. *See* ECF Nos. 186-89. Recognizing that the "conflicting directives from federal courts" to destroy and to preserve the same data "put the government in an untenable position," the FISC granted the Government relief from its earlier destruction order. *See In re Application of the FBI for an Order Requiring the Production of Tangible Things*, BR 14-01, at 5-7 (F.I.S.C. Mar. 12, 2014) (Exh. A, hereto).

After further briefing on the TRO, *see* ECF Nos. 191, 193, 196, this Court "extend[ed] the temporary restraining order . . . until a final order resolving the matter is issued" and ordered that the Government be prohibited from "destroying any potential evidence relevant to the claims

[1] The Government Defendants are filing this memorandum in the *Shubert* action as well.

at issue in this action . . . ." ECF No. 206. The Court also ordered further briefing "[r]egarding the Government's compliance with this Court's prior preservation orders" in this case. *See id.*

Before that briefing was complete, *see* ECF Nos. 229, 233, a second preservation dispute arose. On June 5, 2014, Plaintiffs filed an emergency application for enforcement of the prior TRO to prevent the destruction of communications acquired pursuant to Section 702 of FISA. ECF No. 235. The same day, the Court issued a second TRO, which 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." ECF No 236.

The Government immediately moved to vacate this second TRO, *see* ECF Nos. 243-44. The Court held a hearing on the matter on June 6, 2014, and denied Plaintiffs' motion to enforce the first TRO as to "Section 702 materials," in light of a declaration by the Deputy Director of the NSA describing the operational consequences and the national-security implications of imposing a requirement to preserve all raw Internet communications data acquired through the NSA's Upstream acquisition technique. Minute Order, ECF No. 246; *see* Opp'n to Pls.' Emergency Application to Enforce Court's Temporary Restraining Order, ECF No. 243; Decl. of Richard H. Ledgett, Jr., Deputy Director, NSA, ECF No. 244. Nevertheless, the Court also ordered that the parties brief "[w]hether Plaintiffs' claims encompass Section 702" as well as the "appropriateness of an adverse inference for standing based on the alleged destruction of documents collected pursuant to both Section 215 and 702." Minute Order, ECF No. 246. The parties filed the briefs as directed by the Court in its June 6, 2014 order, and the parties also concluded their briefing on the issue of preservation compliance as ordered by the Court on March 19, 2014. *See* ECF Nos. 253-54, 260. Except as specifically enumerated above, the Court has not ruled on the preservation issues presented in these briefs.

FISA Section 702

Presentation of the preservation issue currently pending before the Court requires a brief discussion of FISA Section 702, NSA Upstream Internet acquisition of Internet communications data pursuant to Section 702, and the recent FISC-approved changes to the manner in which Upstream Internet acquisition is conducted.

Due to changes in communications technology that rendered FISA's traditional legal framework obsolete, Congress enacted the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, to "creat[e] a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad," *Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1144 (2013), without regard to the location of the collection. As relevant here, the FISA Amendments Act added FISA section 702, 50 U.S.C. § 1881a ("Section 702"), which provides that, upon the FISC's approval of a "certification" submitted by the Government, the Attorney General and the Director of National Intelligence ("DNI") may jointly authorize, for a period of up to one year, the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (g). The statute expressly prohibits the targeting of U.S. persons or persons known to be in the United States. *Id.* § 1881a(b).

Four requirements must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, *inter alia*, that a significant purpose of an acquisition is to obtain foreign-intelligence information. *Id.* § 1881a(g)(2)(A)(v), (i)(2)(A). Second, the FISC must find that the Government's "targeting procedures" submitted with the certification are reasonably designed to ensure that any acquisition conducted under the authorization (a) is limited to targeting persons reasonably believed to be located outside the United States, and (b) will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(i)(2)(B). Third, the FISC must find that the Government's "minimization procedures," also submitted with the certification, are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1881a(i)(2)(C); *see also id.* § 1801(h). Fourth, the FISC must also find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). Acquisitions under

Section 702 must be conducted in accordance with FISC-approved targeting and minimization procedures. *Id.* § 1881a(c)(1)(A)).

Upstream Internet Acquisitions of MCTs

Communications of non-U.S. persons are acquired under Section 702 certifications approved by the FISC through the "tasking" of "selectors." A selector is a specific communications facility used by a target, such as an e-mail. The Government tasks a selector by issuing a directive to the appropriate electronic-communications-service provider in the United States to assist the Government in acquiring certain telephone or Internet communications associated with that selector. *See* https://www.pclob.gov/library/702-report.pdf, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014) ("PCLOB Report"), at 7; *see* 50 U.S.C. § 1881a(h). Upstream Internet acquisition is the component of the Section 702 program under which certain electronic communications service providers are compelled to assist the NSA in acquiring communications associated with designated selectors as those communications transit the providers' Internet backbone networks. *See* PCLOB Report, at 35. Of pertinence here, until the changes recently approved by the FISC, Upstream Internet acquisition involved the acquisition not only of communications that are sent to or from a tasked selector, but also of communications "about" a tasked selector. An "about" communication is one that contains references to a targeted selector in the message body, but to which the target may not be a party. *See id.* at 37.

Also of importance here, the NSA's Upstream acquisition of Internet communications is accomplished by acquiring Internet "transactions," packets of data traversing the Internet that together may be understood by a device on the Internet (such as a personal computer) and rendered in an intelligible form to the user of that device. [*Redacted Caption*], 2011 WL 10945618, at *5, 9 n.23 (F.I.S.C. Oct. 3, 2011) ("Oct. 3, 2011 FISC Op."). Internet transactions may contain a single, discrete communication, or multiple discrete communications, and in the latter case are referred to as multiple-communication transactions, or MCTs. *Id.* at *5, 9. Due to technological limitations, the NSA's Upstream Internet acquisition devices are "generally

incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector." *Id.* at *10. "As a practical matter," therefore, the "NSA's [U]pstream collection devices [previously] acquire[d] any Internet transaction transiting the device if the transaction contain[ed] a targeted selector anywhere within it . . . ." *Id.*

In 2011, the FISC articulated certain statutory and constitutional concerns regarding the NSA's handling of certain MCTs. The FISC concluded that, as a result of acquiring certain MCTs, the NSA was acquiring a number of "wholly domestic communications" of U.S. persons, and persons in the United States, "that are not to, from, or about a tasked selector" and are "highly unlikely to have foreign intelligence value." *Id.* at *11, 20. The FISC therefore viewed Upstream Internet acquisition of those certain MCTs as a "substantial intrusion[ ] on Fourth Amendment-protected interests . . . of persons who have little or no relationship to [a] target." *Id.* at *13; *see also id.* at *26. Having reached this conclusion, the FISC initially determined that it could not approve certain portions of the NSA's proposed minimization procedures as consistent with FISA or the Fourth Amendment. *Id.* at *20-21, 28. The FISC therefore ordered the Government either to correct the statutory and constitutional deficiencies it had identified, or cease the acquisition of certain MCTs. *Id.* at *30.

Acting on the FISC's instruction, the Government prepared for the court's review a revised set of minimization procedures to address its concerns regarding acquisition of those certain MCTs. [*Redacted Caption*], 2011 WL 10947772, at *1-2 (F.I.S.C. Nov. 30, 2011) ("Nov. 30, 2011 FISC Op."). These included special segregation, marking, and handling requirements for MCTs; a reduction of the default retention period from five years to two years from the expiration of the certification authorizing the collection, *id.* at *3-5, and a categorical prohibition against analysts' use of "known U.S.-person identifiers to query the results of upstream Internet collection." [*Redacted Caption*], Mem. Op. & Order 18 (F.I.S.C. Apr. 26, 2017) (ECF No. 358-1) ("Apr. 26, 2017 FISC Mem. Op."), at 18, 19 (noting this prohibition was in effect since 2011). The FISC then found that the amended minimization procedures for handling MCTs

"substantially reduce[d] the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated by [the] NSA," and that they "[were] consistent with the requirements of [FISA and] the Fourth Amendment." Nov. 30, 2011 FISC Op., at *6. The FISC accordingly permitted Upstream Internet acquisition to continue under the revised procedures. *Id.* at *8. To avoid issues concerning improper use or disclosure of communications acquired prior to the FISC's approval of the new procedures, the NSA purged all Upstream Internet communications in its repositories that it could determine were collected before the new procedures took effect. [*Redacted Caption*], 2012 WL 9189263, at *3 (F.I.S.C. Aug. 24, 2012).

Recent FISC-Approved Changes to Upstream Acquisition and Mandatory Destruction of Previously Acquired Transactions

The preservation issue now before the Court arose following the Government's submission of its 2016 certifications, and accompanying targeting and minimization procedures, for FISC approval. While the certifications and procedures were still under review, the Government notified the FISC of previously unknown queries of U.S.-person identifiers by NSA analysts in databases containing the NSA's Upstream Internet acquisition, even though NSA minimization procedures since 2011 had expressly prohibited such queries in order to protect U.S.-person information contained in MCTs. *See* Apr. 26, 2017 FISC Mem. Op. at 14-15, 17-19; *see supra*, at 7. Internal NSA reviews indicated that human error was the primary cause of these non-compliance incidents; NSA systems design was also found to be a contributing factor. *See id.* at 20-21. Nevertheless, recalling the concerns expressed by the court in 2011, the FISC considered the situation to be "[a] very serious Fourth Amendment concern[]," *id.* at 19. *See also id.* at 22 (expressing "concern about the extent of non-compliance with important safeguards for interests protected by the Fourth Amendment").

To resolve these compliance problems, in March 2017 the Government submitted a set of amended certifications and revised targeting and minimization procedures that substantially change how the NSA conducts certain aspects of its Upstream Internet acquisition under Section 702. In particular, the Government proposed to eliminate future acquisition of "about"

transactions altogether, in order to avoid the acquisition of potentially problematic MCTs. In addition the Government proposed to sequester and destroy raw Upstream Internet communications data previously collected. *Id.* at 23. As summarized by the FISC, the NSA's amended 2016 minimization procedures[2] require that "all Internet transactions acquired on or before [March 17, 2017] and existing in NSA's institutionally managed repositories [be] sequestered pending destruction such that NSA personnel will not be able to access the[m] for analytical purposes." *Id.* at 23-24 (citing 2016 NSA Minimization Procedures § 3(b)(4)a). The procedures further require that the sequestered transactions be destroyed "as soon as practicable through an accelerated age-off process." *Id.* at 24 (same).

The FISC concluded that these changes to Upstream Internet acquisition "should substantially reduce the acquisition of non-pertinent information concerning U.S. persons," *id.* at 23, that "present[ed] the Court the greatest level of constitutional and statutory concern," *id.* at 28. The "elimination of 'abouts' collection, and consequently, the more problematic forms of MCTs," would sharpen the focus of Upstream Internet acquisition on communications to or from non-U.S. persons outside the United States that are relevant to the NSA's foreign-intelligence mission. *Id.* at 29-30. The FISC therefore approved the Government's amended Section 702 certifications and the accompanying targeting and minimization procedures. *Id.* at 2.[3]

Relevant Proceedings in this Court

On April 17, 2017, the Government submitted its *ex parte, in camera* notice advising the Court of the forthcoming changes to the NSA's Upstream Internet acquisition and their potential impact on preservation matters in this case. *See* ECF No. 349. An unclassified version of the Government's notice was filed on the public record of this case on April 28. *Ex Parte, In*

[2] 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 (Exh. B, hereto) ("2016 NSA Minimization Procedures").

[3] As discussed *infra*, at 13, although the NSA's amended 2016 minimization procedures require the destruction "as soon as practicable" of Upstream Internet transactions acquired on or before March 17, 2017, the procedures make an exception, subject to various conditions, allowing the retention of information that otherwise must be destroyed if it is "subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation." 2016 NSA Minimization Procedures § 3(c)(3); *see* Apr. 26, 2017 FISC Mem. Op. at 24.

Camera Notice of Preservation Matters Potentially Impacted by Changes to NSA Upstream Acquisition [etc.] (ECF No. 350-1) ("Gov't Notice").

The Government's Notice explained that, based on the Court's 2014 denial of Plaintiffs' motion to require preservation of all "702 materials," including all raw Upstream Internet communications, the NSA had continued to age off such communications in accordance with FISC-approved minimization procedures and mission needs. Gov't Notice, at 2-3. The new procedures proposed by the Government, however, would now require the destruction of raw Upstream Internet communications data from the various NSA repositories in which they reside "as soon as practicable." *Id.* at 4. Nevertheless, the Government advised that the NSA would not subject Upstream Internet communications data in its central repository to the accelerated age off process until the resolution by this Court of any challenge by Plaintiffs to the intended destruction of the data. *Id.* at 5. At the May 19, 2017, case management conference the Government sought expedited resolution of any such challenge, so as not to delay unnecessarily the NSA's compliance with the accelerated destruction requirement. The Court accommodated that request by setting a compressed schedule for briefing the issue, *see* Reporter's Tr. of Proceedings, Further Case Management Conference, dated May 19, 2017, at 18, 25, which has since been amended by stipulation and order. *See* Stipulation and Order, ECF No. 364.

Since the May 19 case management conference the Plaintiffs and the Government Defendants have conferred regarding destruction of the legacy Upstream Internet communications data, and the Government proposed to Plaintiffs the approach discussed herein for targeted preservation of communications to or from Plaintiffs' e-mail addresses, if any. To date the parties have not reached agreement, but continue to confer.[4]

[4] The Government has also contacted counsel for the plaintiffs in the companion to this case, *Shubert v. Trump*, No. 4:07-cv-0693-JSW, to ascertain their position regarding destruction of the legacy Upstream Internet communications data. The *Shubert* plaintiffs have not advised the Government whether they consent or object to the destruction, although their counsel has been advised of the proposal for targeted preservation of individual plaintiffs' communications (if any) made to the Plaintiffs in this case. To avoid unnecessarily delaying the NSA's compliance with the accelerated destruction requirement, the Government requests that the Court apply its ruling on preservation of the legacy Upstream Internet communications data in *Shubert* as well. The Government has advised the *Shubert* plaintiffs' counsel of this request and are filing this memorandum in the *Shubert* action as well.

ARGUMENT

I. LITIGANTS' DUTY TO MAKE PRESERVATION EFFORTS THAT ARE REASONABLE AND PROPORTIONAL TO THE NEEDS OF THE CASE.

When litigation is reasonably anticipated against a party, that party has a common law obligation to preserve—*i.e.*, identify, locate, and maintain—information that is "relevant to specific, predictable, and identifiable litigation." *Apple Inc. v. Samsung Elec. Co.,* 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012). "It is well-established that the duty pertains only to relevant documents." *Id.* (collecting cases). "Relevant" in this context means relevant for purposes of discovery, *see, e.g.*, Fed. R. Civ. P. 26(b)(1), 34(a)(1), including information that relates to the claims or defenses of any party. Fed. R. Civ. P. 26(b)(1).

Once the duty to preserve takes effect, the preserving party is "required to suspend any existing policies related to deleting or destroying files and preserve all relevant documents related to the litigation." *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006); *Apple Inc.*, 881 F. Supp. 2d at 1137. The common law duty to preserve relevant, discoverable information persists throughout the litigation. *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

Reasonableness and proportionality are recurring touchstones informing the extent of a party's preservation obligations. *See Apple Inc.*, 881 F. Supp. 2d at 1137 n.26, 1144; *Starline Windows Inc. v. Quanex Bldg. Prod. Corp.*, 2016 WL 4485568, at *9 (S.D. Cal. Aug. 19, 2016), quoting *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522 (D. Md. 2010). Because the duty to preserve "is neither absolute, nor intended to cripple organizations," *Victor Stanley, Inc.*, 269 F.R.D. at 522 (citation omitted), determining whether preservation conduct is acceptable in a given case "depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case." *Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010); *see also Rogers v. Averitt Express, Inc.*, 215 F. Supp. 3d 510, 516 (M.D. La. 2017) (quoting *Rimkus* with approval); *Zbylski v. Douglas Cty. Sch. Dist.*, 154 F. Supp. 3d 1146, 1164 (D. Colo. 2015) (same); *Little Hocking Water Assn., v. E.I. du Pont de Nemours & Co.*, 94 F. Supp. 3d 893, 918 (S.D. Ohio 2015)

("[T]he scope of the duty to preserve is a highly fact-bound inquiry that involves considerations of proportionality and reasonableness.") (citation omitted).

Because "[p]reservation and production are necessarily interrelated," application of the proportionality and reasonableness principles to preservation "flows from the existence of th[ose] principle[s] under the Federal Rules of Civil Procedure." *Pippins v. KPMG LLP*, 279 F.R.D. 245, 255 (S.D.N.Y. 2012); Fed. R. Civ. P. 37(e) Advisory Comm. Notes to 2015 Amendments ("Another factor in evaluating the reasonableness of preservation efforts is proportionality. . . . [A]ggressive preservation efforts can be extremely costly, and parties (including government parties) may have limited staff and resources to devote to those efforts."). To that end, Rule 26's "'proportionality' test for discovery" applies to the preservation context. *Pippins*, 279 F.R.D. at 255.[5] Rule 26(b)(1) states that a party may only obtain discovery that is "proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26(b)(1); U.S. District Court for the Northern District of California, Guidelines for the Discovery of Electronically Stored Information ("ESI"), Guideline 1.03 ("The proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) . . . should be applied to," *inter alia*, "the preservation . . . of [electronically stored information (ESI)]."); Guideline 2.01(b) ("The parties should strive to define a scope of preservation that is proportionate and reasonable and not disproportionately broad, expensive, or burdensome.").[6]

[5] The *Pippins* decision grounded this proportionality test entirely in Rule 26(b)(2)(C)(iii). *Pippins*, 279 F.R.D. at 255. Since *Pippins* was decided, Rule 26 has been amended to place the proportionality test in Rule 26(b)(1), a move designed to "reinforce" the centrality of proportionality to discovery, but that "does not change the existing responsibilities of the court and the parties to consider proportionality." Fed R. Civ. P. 26 Advisory Comm. Notes to 2015 Amendments.

[6] *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"); Fed. R. Civ. P. 26 Advisory Comm. Notes to 2015 Amendments ("Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available.").

For this reason, courts considering a party's preservation obligations, including whether additional preservation measures are necessary, balance the burden of preserving certain information with the moving party's showing of its relevance. *See, e.g.*, *City of Wyoming v. Procter & Gamble Co.*, 2016 WL 6908110, at *2 (D. Minn. Oct. 7, 2016) ("In determining whether a preservation order should be entered, . . . [t]his Court is additionally guided by . . . the proportionality principles of Rule 26(b)(1)."); *Martinelli v. Johnson & Johnson*, 2016 WL 1458109, at *2 (E.D. Cal. Apr. 13, 2016); *FTC v. DirecTV, Inc.*, 2016 WL 7386133 (N.D. Cal. Dec. 21, 2016) (concluding court could not sanction party for failing to preserve certain information given Rule 26(b)(1)'s proportionality principle); *In re Broiler Chicken Antitrust Litig.*, 2017 WL 1682572, at *6 (N.D. Ill. Apr. 21, 2017) (concluding, even though requested preservation would "increase the likelihood that relevant information . . . is not destroyed," party had failed to show it was "proportional to the needs of the case and consistent with judicial efficiency and economy.").

II. THE GOVERNMENT'S PROPOSAL FOR TARGETED PRESERVATION OF LEGACY UPSTREAM COMMUNICATIONS THAT ARE TO OR FROM THE PLAINTIFFS (IF ANY) CONSTITUTES A REASONABLE AND PROPORTIONAL APPROACH TO THE PRESERVATION OF POTENTIALLY RELEVANT EVIDENCE.

The NSA's FISC-approved minimization procedures require the Government to sequester and destroy "as soon as practicable" all Internet transactions acquired "by upstream Internet collection under Section 702" on or before March 17, 2017 that exist in the "NSA's institutionally managed repositories" and then "submit written updates" to the FISC every 90 days about the Government's implementation of this process. Apr. 26, 2017 FISC Mem. Op. at 23-24, 98. This destruction requirement is arguably subject to a narrow exception that the "NSA may retain specific section 702-acquired information" if it is "subject to a preservation obligation in pending . . . civil . . . litigation." 2016 NSA Minimization Procedures § 3(c)(3); *see also* Apr. 26, 2017 FISC Mem. Op. at 24. Although in 2014 the Court denied Plaintiffs' motion to require the Government to preserve "all Section 702 materials," including raw Upstream Internet communications data, *see supra* at 4, and the Government Defendants continue to take the position that no preservation obligations currently exist regarding legacy Upstream Internet

communications data, they nevertheless propose a reasonable and proportional approach that would allow for the destruction of the vast majority of that data while preserving communications involving the Plaintiffs, if any, that are contained therein.

Specifically, the Government Defendants propose that the Court order:

- That the *Jewel* and *Shubert* Plaintiffs provide to the Government the e-mail addresses that they have used since 2014 (an outer bound on the date range of the legacy Upstream Internet communications data), and the dates during which they used those addresses;
- That the NSA take those steps necessary to identify and preserve any Upstream Internet communications data to or from the e-mail addresses identified by Plaintiffs, if any such communications containing those e-mail addresses exist in the legacy Upstream Internet communications data contained in the NSA's central repository;
- That the NSA sequester any Upstream Internet communications of Plaintiffs identified through the process described above for the pendency of the respective actions, such that neither the NSA nor any other agency would have analytic access to those communications, with only technical access permitted for purposes of maintaining data integrity and such other access as may be needed for purposes of this litigation;
- That, because the identification of Plaintiffs' communications contained in the legacy Upstream Internet communications data, if any, would involve access to that information arguably in contravention of NSA's FISC-approved Section 702 minimization procedures, the Government first notify the FISC of the Court's order, and notify this Court of any objections raised by the FISC, before proceeding as described;
- That nothing in the Court's order itself is to be construed as requiring the Government to inform Plaintiffs, or otherwise publicly state, whether or not any of Plaintiffs' communications were located in the legacy Upstream Internet communications data, the existence or non-existence of such communications being a classified fact; and
- That the Government Defendants, upon completion of the identification described above and the sequestration, as described above, of any communications of Plaintiffs identified as a result, will be under no obligation to preserve any other legacy Upstream Internet communications data for purposes of the *Jewel* and *Shubert* cases.

Of course, this process cannot begin until Plaintiffs furnish the Government with their respective e-mail addresses. To date, they have not done so.

Preserving Plaintiffs' e-mails (if any) that may currently exist in the NSA's central repository, while allowing for the destruction of the remainder of all Internet transactions acquired by the NSA's Upstream Internet acquisition technique under Section 702 on or before

March 17, 2017, is a reasonable and proportional approach to resolving the preservation dispute between the parties. *See, e.g.*, *Starline Windows, Inc.*, 2016 WL 4485568, at *9 ("Whether preservation . . . conduct is acceptable in a case depends on what is *reasonable*, and that in turn depends on whether what was done—or not done—was *proportional* to that case . . . .").

First, this approach is reasonable and proportional because any e-mails involving Plaintiffs would constitute readily identifiable communications whose presence (if any) in the NSA's central repository of legacy Upstream Internet communications would be relevant to the question of Plaintiffs' standing to challenge FISC-authorized Upstream Internet acquisition as a violation of the Wiretap Act. An e-mail communication is an unclassified (and thus workable) example of a selector that can be used to identify specific communications involving Plaintiffs that were acquired (if any) under the NSA's Upstream Internet acquisition technique. *See* PCLOB Report, at 7.

Second, this approach is reasonable and proportional in light of the fact that the Government is also already preserving other information about the NSA's Upstream Internet acquisition technique. Notwithstanding the Government's disagreement with Plaintiffs' stated position that the allegations in their complaint encompass FISC-authorized activities such as Upstream Internet acquisition, *see, e.g.*, ECF No. 229, at 13-26, the Government Defendants have implemented litigation holds to preserve documents that reflect the scope of Upstream Internet communications acquisition and the manner in which it is conducted.
These documents include certifications, targeting and minimization procedures, and directives issued to electronic communications service providers under Section 702, as well as submissions made to the FISC under Section 702.

Third, the Government's proposed approach is also reasonable and proportional given that almost all information that the Government has preserved and is proposing to preserve regarding the NSA's Section 702 Upstream Internet acquisition technique remains classified and cannot be publicly disclosed without risking exceptionally grave damage to national security, *see, e.g.*, Decl. of James R. Clapper, Director of National Intelligence, ECF No. 168, ¶¶ 33-34 (whether Plaintiffs' communications are subject to NSA intelligence-gathering activities is

classified), ¶¶ 42-43 (identity of providers who are compelled to assist NSA is classified). Indeed, this Court—in granting summary judgment for the Government Defendants in Plaintiffs' Fourth Amendment challenge to the same Upstream Internet acquisition technique that is the subject of this preservation dispute—has already held that the information at issue is subject to the state secrets privilege. *See Jewel v. NSA*, 2015 WL 545925, at *2 (N.D. Cal. Feb. 10, 2015) ("[T]he Court finds that the . . . Fourth Amendment Claim would have to be dismissed on the basis that any possible defenses would require impermissible disclosure of state secret information."); *id.* at *5 ("Because a fair and full adjudication of the Government Defendants' defenses would require harmful disclosures of national security information that is protected by the state secrets privilege, the Court must exclude such evidence from the case.").

For these reasons, a targeted approach to preservation is reasonable and proportional to the needs of this case.

III. WHOLESALE PRESERVATION OF LEGACY UPSTREAM DATA WOULD UNNECESSARILY CONTRAVENE EFFORTS BY THE NSA AND THE FISC TO PROTECT IMPORTANT FOURTH AMENDMENT INTERESTS AND WOULD BE NEITHER REASONABLE NOR PROPORTIONAL.

As noted above, the NSA's legacy Upstream Internet communications data includes certain MCTs that have presented "the greatest level of constitutional and statutory concern" to the FISC. *See* Apr. 26, 2017 FISC Mem. Op. at 28. Notwithstanding the sequestration of these communications (as required by the amended 2016 minimization requirements, *see* 2016 NSA Minimization Procedures § 3(b)(4)a), the continued retention of those communications implicates substantial Fourth Amendment interests. *See* Oct. 3, 2011 FISC Op., at *19, 20-21, 22, 28.

To safeguard against the risk of infringing on the constitutionally protected privacy interests of U.S. persons whose communications are contained among the legacy Upstream Internet communications data, those communications should be destroyed "as soon as practicable," as the NSA's amended 2016 minimization procedures require. *See* 2016 NSA Minimization Procedures § 3(b)(4)a. And, while the minimization procedures include an exception allowing retention of specific information to comply with preservation obligations,

that exception should not be invoked to preserve wholesale every one of the legacy Upstream Internet communications data in light of the Fourth Amendment interests that the FISC (exercising its oversight role) has endeavored to defend, and that the Government also wishes to respect. Additionally, to mandate preservation of all of that data would be neither reasonable, nor proportional to the needs of these cases, *see Starline Windows, Inc.*, 2016 WL 4485568, at *9, given that the data contains communications by U.S. persons that have nothing to do with the Plaintiffs in this case, or in *Shubert*, and thus that could have no relevance to the issues in either case.

CONCLUSION

For the foregoing reasons, the Court should adopt the scheme for targeted preservation of legacy Upstream Internet communications data proposed by the Government, and it should not require the preservation of all legacy Upstream Internet communications data in the NSA's central repository, or otherwise delay the accelerated age off of that data.

DATE: June 13, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
RODNEY PATTON
Senior Counsel

JULIA A. BERMAN
CAROLINE J. ANDERSON
TIMOTHY A. JOHNSON
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Rm. 7320
Washington, D.C. 20001
E-mail: rodney.patton@usdoj.gov
Phone: (202) 305-7919
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities