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

Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

VIRGINIA SHUBERT, *et al.*,

Plaintiffs,

v.

BARACK OBAMA, *et al.*,

Defendants.

Case No. 4:08-cv-04373-JSW
Case No. 4:07-cv-00693-JSW

ERRATA TO THE GOVERNMENT DEFENDANTS' REPLY BRIEF REGARDING COMPLIANCE WITH PRESERVATION ORDERS

No hearing scheduled
Oakland Courthouse
Courtroom 5, 2nd Floor
The Honorable Jeffrey S. White

The Government Defendants submit this Errata, which accompanies a corrected version of their Reply Brief Regarding Compliance With Preservations Orders, in order to detail the non-substantive differences between the version of this submission, originally filed on June 27, 2014 (*Jewel* ECF No. 253, *Shubert* ECF No. 134), and the corrected version filed herewith:

1. A Table of Contents and Table of Authorities have been added.

Dated: June 30, 2014

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
JULIA BERMAN
julia.berman@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Attorneys for the Government Defendants Sued in their Official Capacities

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

Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-04373-JSW Case No. 4:07-cv-00693-JSW **GOVERNMENT DEFENDANTS' REPLY BRIEF REGARDING COMPLIANCE WITH PRESERVATION ORDERS** No hearing scheduled Oakland Courthouse Courtroom 5, 2nd Floor The Honorable Jeffrey S. White
VIRGINIA SHUBERT, *et al.*, Plaintiffs, v. BARACK OBAMA, *et al.*, Defendants.	

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

INTRODUCTION

The Government has always understood this litigation, and therefore its preservation obligations, to concern alleged National Security Agency (NSA) surveillance programs carried out under presidential, not statutory or judicial, authority. Plaintiffs now assert that they always meant to contest NSA intelligence-gathering activities conducted under statutory and judicial authority—specifically, under orders issued by the Foreign Intelligence Surveillance Court (FISC) pursuant to the Foreign Intelligence Surveillance Act (FISA). However, only the Government's view of the litigation's scope can be reconciled with the instruments that define that scope—the complaints, which do not challenge FISC-authorized programs. Rather, both complaints clearly state that Plaintiffs take issue with presidentially authorized intelligence programs, not regardless of, but *because of* the fact that the activities alleged were conducted under presidential, not judicial or statutory, authority. Because the fundamental premise of Plaintiffs' claims in these cases is a *lack* of statutory authority or judicial approval, and because the complaints otherwise do not purport to challenge programs conducted pursuant to statutory authority, Plaintiffs' attacks on the Government's preservation of information concerning FISC-authorized, FISA-based programs must fail under any fair reading of the complaints.

As directed by the Court at the close of the March 19, 2014, hearing, the Government detailed in its opening brief the extensive steps taken by the NSA, and other involved agencies, to preserve information relevant to the programs at issue in these cases: presidentially authorized NSA intelligence programs initiated in the wake of the 9/11 attacks. In response, Plaintiffs do not contest the sufficiency of these efforts. Rather, they assert that the Government also has been obligated to undertake similar efforts regarding FISC-authorized intelligence programs that are not challenged (or otherwise alluded to) in the complaints; that the Government breached this duty when it complied with FISC orders limiting the retention of communications information collected under these statutorily based programs; and that the Government should be sanctioned for spoliation by an adverse inference that effectively presumes Plaintiffs' standing to sue.

Following the June 6, 2014, hearing at which the Court denied Plaintiffs' emergency motion to enforce the Court's March 10, 2014, temporary restraining order, the Court issued a minute order also directing the parties to address, in further briefing, the following issues:

(1) whether Plaintiffs' claims encompass surveillance activities conducted under FISA Section 702, and the scope of the collection activities under that provision; and

(2) the appropriateness of an adverse inference of standing based upon the alleged destruction of documents collected pursuant to both Section 215 of the USA Patriot Act and Section 702.

The Government addresses all of these matters herein, and demonstrates that Plaintiffs' claims regarding preservation lack merit and that no relief is warranted. First, as explained below, surveillance under Section 702 involves targeting non-U.S. persons located abroad, and thus bears no resemblance to the mass surveillance of millions of Americans' communications alleged in the complaints. Second, nothing to which Plaintiffs point in their complaints, or any other filings, can reasonably be taken as notification to the Government that Plaintiffs' claims (and, thus, the Government's preservation obligations) encompass NSA intelligence programs authorized under FISA, including surveillance conducted under Section 702. Third, the Government's compliance with FISC-ordered limits on the retention of communications information collected under these programs—limitations imposed to protect individual privacy, and ensure the programs' legality—cannot meaningfully be characterized as spoliation. Plaintiffs certainly have made no showing of fault by the Government or prejudice to their case that could justify their request for a conclusive presumption of this Court's jurisdiction under Article III.

In short, the Government has met its preservation obligations in these cases as defined under any reasonable reading of the complaints. No greater preservation efforts on the Government's part are or have been necessary, or should now be required.

ARGUMENT

I. COLLECTION UNDER SECTION 702 IS TARGETED AT NON-U.S. PERSONS LOCATED ABROAD, AND BEARS NO RESEMBLANCE TO THE MASS SURVEILLANCE OF MILLIONS OF AMERICANS' COMMUNICATIONS ALLEGED IN THE COMPLAINTS.

A. Statutory Framework of Section 702 of FISA

Congress enacted the Foreign Intelligence Surveillance Act ("FISA") in 1978 to authorize and regulate certain governmental surveillance of communications and other activities for purposes of gathering foreign intelligence.[1] Section 702 of the FISA, codified at 50 U.S.C. § 1881a, was enacted in 2008 as part of the FISA Amendments Act of 2008, *see* Pub L. No. 110-261, sec. 101(a)(2), § 702, 122 Stat. 2438, and "was widely and publicly debated in Congress both during the initial passage in 2008 and the subsequent reauthorization in 2012." NSA Director of Civil Liberties and Privacy Office Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Apr. 16, 2014) ("Civil Liberties and Privacy Office Report") (attached as Exhibit A, hereto) at 2.

The statute authorizes only the targeting of specific *non-U.S. persons*[2] who are reasonably believed to be *located outside* the United States to acquire communications associated with those persons who have been determine to possess or are likely to receive foreign intelligence information. *See* 50 U.S.C. § 1881a(a), (b)(1), (3). The Government does not and cannot indiscriminately collect communications in bulk under Section 702, and thus the statute does not authorize a "dragnet" surveillance of American citizens. *See id.* § 1881a. To the contrary, under the express terms of Section 702, the Government "may not intentionally target any person known at the time of acquisition to be located in the United States," "may not intentionally target a United States person reasonably believed to be located outside the United States," "may not intentionally target a person reasonably believed to be located outside the

[1] In enacting FISA, Congress also created the Foreign Intelligence Surveillance Court ("FISC"), an Article III court of 11 appointed U.S. district judges with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of intelligence-gathering by the Government. *See* 50 U.S.C. § 1803(a); *see In re Motion for Release of Court Records*, 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

[2] The term "United States person" includes citizens of the United States, aliens admitted for permanent residence, and certain associations and corporations. *See* 50 U.S.C. § 1801(i).

United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States"; and "may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States." *Id.* § 1881a(b).

Section 702 does not require an individualized court order addressing each non-United States person to be targeted under its provisions. However, except in "exigent circumstances,"[3] before the Government may target foreign persons abroad under this statute, the Attorney General and the Director of National Intelligence ("DNI") annually must seek approval from the FISC of a written certification (with supporting affidavits as appropriate) that identifies categories of foreign intelligence information to be acquired by the Government through the targeting of non-United States persons abroad. The FISC must also approve the use of targeting and minimization procedures. *See id.* §§ 1881a(a), (d), (e), (g) & (i)(3). To approve the certification, the FISC must find that it contains all the required elements set out in § 1881a(g), including that "a significant purpose of the acquisition is to obtain foreign intelligence information" and that "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider." *Id.* § 1881a(g)(2)(A)(v), (vi); *id.* § 1881a(i)(2)(A). In order to approve the use of targeting procedures, the FISC must find that the procedures are reasonably designed to ensure that any acquisition conducted under the certification is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. The FISC must also find the procedures consistent with the Fourth Amendment. *See id.* §§ 1881a(i)(2)(B), (3)(A).

In addition, even though U.S. persons may not be targeted for acquisitions under Section 702, *see id.* § 1881a(b), the statute requires the Government to adopt, and the FISC to approve,

[3] The Attorney General and the DNI may authorize targeting to commence under Section 702 before the FISC issues its order if they determine that certain "exigent circumstances" exist, 50 U.S.C. § 1881a(a), (c)(2). If that determination is made, the Attorney General and the DNI must, within seven days, submit for FISC review their certification, including the targeting and minimization procedures used in the acquisition. *See id.* § 1881a(g)(1)(B); *see also id.* § 1881a(d), (e), (g)(2)(B).

minimization procedures that must be "reasonably designed in light of the purpose and technique of the particular surveillance 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.* § 1801(h), and be consistent with the Fourth Amendment. *See id.* § 1881a(i) (2)(C) , (3) (A).

Once the FISC has found that the certification from the Attorney General and the DNI contains all the required elements and that the targeting and minimization procedures are consistent with the statutory requirements and the Fourth Amendment, the FISC "shall enter an order approving the certification and the use" of "the procedures for the acquisition" of foreign intelligence information under the statute. *See id.* § 1881a(i)(3)(A).[4]

B. Operation and Scope of the Section 702 Program

Multiple federal agencies (NSA, CIA, and the FBI) participate in the Section 702 collection program, *see* [redacted caption] Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *6-8, but NSA takes the lead in "targeting" and "tasking." *See* Intelligence Community's Collection Programs under Title VII of the Foreign Intelligence Surveillance Act ("IC's Collection Programs") (attached as Exhibit B, hereto) at 3. The Section 702 targeting process begins with the NSA identifying, in accordance with the FISC-approved procedures, a target—a non-U.S. person located outside the United States who has been and/or is likely to communicate foreign intelligence information as designated in a certification by the Attorney General and the DNI.

[4] In addition to mandating the FISC's role in approving the certification, Section 702 provides for continuing oversight by the FISC, the judiciary and intelligence committees of both houses of Congress, and the inspectors general of the Department of Justice and each element of the Intelligence Community, of the Government's compliance with approved targeting procedures and its use of any information concerning U.S. persons collected through Section 702 acquisitions. *See* 50 U.S.C. § 1881a(l). For example, the statute requires that the Attorney General and the DNI adopt guidelines to train intelligence personnel regarding the implementation of targeting restrictions, which must be provided to Congress and the FISC, *see id.* § 1881a(f)(1); the Attorney General and the DNI must assess the Government's compliance with the pertinent targeting and minimization procedures semi-annually and these assessments must be submitted to Congress and to the FISC, *see id.* § 1881a(l); and each element of the Intelligence Community that conducts Section 702 acquisitions must report annually to the DNI, the Attorney General, Congress, and the FISC concerning their use of information obtained through the acquisitions. *See id.* § 1881a(l)(3).

See Civil Liberties and Privacy Office Report at 4. The NSA analyst "attempts to determine how, when, with whom, and where the target communicates," so the target's "unique identifier" (such as a telephone number or e-mail address) can be used as a selector. *See id.*[5] Following an internal review to ensure that the proposed targeting is consistent with the targeting procedures, *see id.* at 5, the Government may "task" the target's "selector" by directing the appropriate electronic communications service provider in the United States to assist the Government in acquiring certain telephone or Internet communications involving that selector. *See* 50 U.S.C. § 1881a(b); Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *5-6, 29; Civil Liberties and Privacy Office Report at 5. In response to these taskings, the NSA receives information concerning tasked selectors through two different methods, one generally referred to as "PRISM collection" and the other generally referred to as "upstream collection." Civil Liberties and Privacy Office Report at 5.[6]

PRISM "is an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers." Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Office of the Director of National Intelligence (June 8, 2013) ("DNI Fact Sheet") (attached as Exhibit D, hereto) at 1. Under PRISM collection, the "Government provides selectors to service providers through the FBI" and the service

[5] The Office of the Director of National Intelligence ("ODNI") recently released a statistical transparency report regarding the use of various national security authorities, including Section 702. *See* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Annual Statistics for Calendar Year 2013* (attached as Exhibit C, hereto). In that report, the estimated number of foreign targets affected by Section 702 legal authority in 2013 was 89,138. *See id.* at 1.

[6] Communications acquired by the NSA under authority of Section 702 are "processed and retained in multiple NSA systems and data repositories." Civil Liberties and Privacy Office Report at 6. As one example of how this information is handled by a recipient, NSA analysts "access the information via 'queries'" that are designed to "return valid foreign intelligence and minimize[] the likelihood of returning non-pertinent U.S. person information." *Id.* at 6-7. Importantly, "[a]ccess" to these systems and repositories "is controlled, monitored, and audited." *Id.* at 7. Since October 2011, the FISC has approved the NSA's use of "U.S.-Person identifiers" to query the PRISM data—but not the "fruits of NSA's upstream collection"—so long as the query is "reasonably likely to yield foreign intelligence information" and also otherwise complies with the FISC-approved minimization procedures. Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *7 & n.21; Civil Liberties and Privacy Office Report at 7.

providers furnish the "NSA with communications to or from these selectors." Civil Liberties and Privacy Office Report at 5; *see also* IC's Collection Programs at 3. The "NSA also can designate the communications from specified selectors acquired through PRISM collection to be 'dual-routed' to other Intelligence Community elements," each of which must have its own minimization procedures that have been approved by the FISC. *See* IC's Collection Programs at 4.[7] The "vast majority" of the "more than two hundred fifty million Internet communications" collected pursuant to Section 702 in 2011, for example, were collected under PRISM directly from service providers and were "discrete Internet communications," Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *9, involving the targeted selectors. Civil Liberties and Privacy Office Report at 5.[8]

In addition to collecting information directly from the service providers, Section 702 authority also allows NSA to collect certain "telephone and electronic communications" through its "upstream collection," *id.*, as those communications "transit the Internet 'backbone' within the United States." IC's Collection Programs at 3. The NSA's upstream collection is "small in relative terms," Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *10, in that in 2011 it acquired only "approximately 9%" (roughly 22 million) "[out] of the total Internet communications acquired by the NSA under Section 702." *Id.* at *7 n.21; *see id.* at *9 n.24. Upstream collection, however, allows the NSA's acquisition of electronic communications not only to and from the targeted e-mail address but also the acquisition of Internet communications that contain

[7] These agencies can retain and disseminate information acquired under this PRISM collection only in accordance with those procedures, which must be reasonably designed to minimize the acquisition and retention, and to prohibit the dissemination, of private information concerning U.S. persons consistent with the Government's need to obtain, produce, and disseminate foreign intelligence information. *See* 50 U.S.C. § 1801(h). "The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications." Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *6 n.17; *see also id.* at *8 n.22.

[8] "According to figures published by a major [technology services] provider, the Internet carries 1,826 Petabytes of information per day." The National Security Agency: Missions, Authorities, Oversight and Partnerships (Aug. 9, 2013) (attached as Exhibit E, hereto) at 6. In fulfilling its foreign intelligence mission under *all* applicable authorities (of which Section 702 is only one), NSA touches about 1.6% of that traffic. *See id.* So, if the size of a basketball court represents the global communications environment, the "NSA's total collection would be represented by an area smaller than a dime on that basketball court." *Id.* And NSA analysts look at much less, only "0.00004% of the world's [Internet] traffic." *Id.*

references to a targeted selector in the bodies of the communications, that is, communications that are "about" the targeted selector. *See* IC's Collection Programs at 4.

The "NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet 'transactions,'" Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *5. An Internet transaction can be either a single discrete communication or multiple discrete communications ("multiple-communication transactions" or "MCTs") only one of which contains a targeted selector. *Id.* at *9.[9] "NSA's upstream collection 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. This means that "NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it," *id.*, that is, if the transaction contains a communication that is to, from, or about the targeted selector. *See id.* at *27. Nevertheless, in evaluating the lawfulness of the NSA's upstream collection in 2011, the FISC "accept[ed] the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection." Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *20. And the FISC also "accept[ed] the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector." *Id.*

Consistent with the requirements of FISA and the Fourth Amendment, the Attorney General has adopted (and the FISC has approved) minimization procedures that the Government is obligated to follow which must be "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the

[9] An "Internet 'transaction'" is "'a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.'" Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *9 n.23 (quoting Government's June 1, 2011 Submission to FISC). In contrast to its upstream collection, the NSA does not acquire Internet "transactions" through its PRISM collection. *See id.* at *9 n.24.

dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h); *see also id.* §§ 1881a(e), (i)(2)(C); *see also, e.g.*, 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 ("NSA Minimization Procedures") (attached as Exhibit F, hereto). The FISC has approved these procedures, including the procedures the NSA specifically adopted to address the incidental collection of certain communications involving U.S. persons under the NSA's upstream collection program. *See* [redacted caption] Aug. 24, 2012 FISC Op., 2012 WL 9189263, at *2-3; [redacted caption] Nov. 30, 2011 FISC Op., 2011 WL 10947772, at *3-6.[10]

These procedures are too numerous to detail here. Most pertinent for current purposes, however, the minimization procedures generally prohibit retention of raw (unminimized) communications obtained via PRISM collection any longer than "five years from the expiration date of the certification authorizing the collection." NSA Minimization Procedures at 7; *see also* Civil Liberties and Privacy Office Report at 8. Similarly, information obtained via upstream collection "may be retained no longer than two years from the expiration date of the certification authorizing the collection." NSA Minimization Procedures at 7; *see also* Civil Liberties and Privacy Office Report at 8.[11] Indeed, having previously declared that the NSA's then-proposed

[10] The FISC found that, "[t]aken together, these [newly adopted] measures for handling Internet transactions tend to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated by the NSA." Nov. 30, 2011 FISC Op., 2011 WL 10947772, at *6.

[11] This brief describes only a few of the NSA's minimization procedures. Additional procedures and compliance requirements that apply to a variety of circumstances 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 the target's status (determined to be a U.S. person), attorney-client communications, "domestic communications," and "foreign communications of or concerning United States persons." NSA Minimization Procedures at 7-9. This section of the brief, which addresses the scope of Section 702 collection, also does not detail the minimization procedures as they apply to the dissemination, in an NSA foreign intelligence report, of U.S. person information. Briefly, under the NSA's minimization procedures, dissemination "is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury." Civil Liberties and Privacy Office Report at 7; *see also* NSA

minimization procedures—including a five-year retention policy for upstream collection—were deficient on statutory and constitutional grounds, the FISC stated in 2011 that the NSA's now-current two-year retention period was integral to its decision to re-approve the NSA's program under Section 702 as consistent with the Fourth Amendment. *See* Nov. 30, 2011 FISC Op., 2011 WL 10947772, at *6.[12]

In short, the Section 702 program is restricted by law to targeting non-U.S. persons located overseas. It is not a "dragnet" program of mass surveillance of Americans' telephonic and online communications.

II. NOTHING IDENTIFIED BY PLAINTIFFS IN THEIR COMPLAINTS OR IN THE PARTIES' OTHER FILINGS CAN REASONABLY BE UNDERSTOOD TO INDICATE THAT PLAINTIFFS CONTEST THE LEGALITY OF FISC-AUTHORIZED INTELLIGENCE PROGRAMS.

In its opening brief, the Government detailed the steps it has taken to preserve documents and information related to the NSA intelligence activities authorized by President Bush after 9/11 that may be relevant to Plaintiffs' claims. Government Defendants' Brief Regarding Compliance with Preservation Orders at 26-30 (ECF No. 229) ("Gov't Defs.' Opening Brief").[13] Plaintiffs do not take issue with the sufficiency of these efforts. Rather they argue exclusively that the Government is also required to preserve documents and information related to FISC-authorized, FISA-based, intelligence programs, including communications information collected under those programs. These arguments are meritless.

Minimization Procedures at 8-11; IC's Collection Programs at 4. Even if one of these conditions applies, however, NSA "may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically 'masks' the true identities of U.S. persons through use of such phrases as 'a U.S. person'" instead of the person's name or other identifying characteristics. Civil Liberties and Privacy Office Report at 7.

[12] The assertion made by Plaintiffs' counsel during the June 6, 2014, hearing, that the Section 702 program is one part of the "dragnet" collection of the content of Americans' communications alleged in the complaints, is without foundation. As the Government has explained in numerous sworn declarations filed in these cases, Plaintiffs' allegations that the NSA was authorized after the September 11, 2001, attacks to engage in indiscriminate collection of the content of millions of Internet-based and telephonic communications are false. *E.g.*, Classified Declaration of Frances J. Fleisch (unclassified public version) (ECF No. 172-8), ¶ 6.

[13] Citations herein to "ECF No. ___" refer to the Court's electronic docket in *Jewel v. NSA*, No. 08-cv-4373-JSW, unless otherwise indicated.

As demonstrated by the Government in its opening brief, it correctly understood that Plaintiffs' complaints challenge NSA intelligence activities not authorized by any statute or court, and thus do not encompass activities specifically authorized by the FISC; the Government certainly had no reasonable notice to the contrary. Gov't Defs.' Opening Brief at 13-26. Plaintiffs' complaints allege facts about presidentially authorized intelligence activities, not FISC-authorized activities, and specifically claim they were unlawful because they were not authorized by any statute or court. In particular, the targeting of communications under Section 702 of FISA involves publicly disclosed programs that Plaintiffs have long known about yet failed to challenge in their complaints. It is perfectly understandable that they did not do so, because, as discussed above, Section 702 authorizes only targeted surveillance of non-U.S. persons, whereas Plaintiffs have always challenged alleged mass surveillance of Americans. Accordingly, Plaintiffs' contention that their complaints encompass FISC-authorized activities, and that the Government was therefore obligated to preserve documents and information regarding those activities, should be rejected.

In response, Plaintiffs claim that any references in their complaints to the lack of judicial or statutory authorization for the challenged NSA intelligence activities are simply suggestive of a potential defense, not an element of their claims. Pls.' Brief Re: The Gov't Defs.' Non-Compliance With the Court's Evidence Preservation Orders at 10 (ECF No. 233) ("Pls.' Brief"). But the complaints make clear this is not so. Under any fair reading of the complaints, the contention that the alleged intelligence activities were authorized by President Bush, and not by any statute or court, is pled as an essential fact, not alluded to as a potential defense.

The *Jewel* complaint, under the heading "Factual Allegations Related to All Counts," contains an entire series of allegations on "The President's Authorization of the Program." *Jewel* Compl. ¶¶ 39-49. It starts by alleging that "[o]n October 4, 2001, President Bush . . . issued a secret presidential order (the "Program Order") authorizing a range of surveillance activities inside of the United States without statutory authorization or court approval, including electronic surveillance of Americans' telephone and Internet communications (the "Program")." *Id.* ¶ 39. The complaint continues that "[t]he President renewed and, on information and belief, renews his

October 4, 2001 order approximately every 45 days." *Id.* ¶ 41. It also alleges that the assistance of telecommunications companies is obtained "based on periodic written requests from Defendants . . . indicating that the President has authorized the Program's activities …," rather than by court order. *Id.* ¶ 42.[14]

The *Shubert* complaint similarly contains numerous factual allegations about a presidentially authorized "Spying Program." *See, e.g., Shubert* 2d Am. Compl. ¶ 57 ("On or around October 4, 2001, President Bush issued an order authorizing the NSA to conduct surveillance of telephone and Internet communications of persons within the United States, without court-approved warrants or other judicial authorization. . . . 'After 9/11 . . . top officials in the [Bush] administration dealt with FISA the way they dealt with other laws they didn't like: They blew through them in secret ….'"); *id.* ¶ 58 (describing Presidential orders authorizing the "Spying Program"); *id.* ¶ 60 (describing legal opinions in support of the "Spying Program"); *id.* ¶ 61 (alleging the Program operates in lieu of court orders or other judicial authorization); *id.* ¶¶ 97-98 (discussing presidential reauthorization of the Program in March 2004).

Thus, the complaints do not merely allege in passing that the activities were conducted "'without judicial or other lawful authorization,'" as Plaintiffs contend. Pls.' Brief at 12-13 (quoting *Jewel* Compl. ¶¶ 76, 92, 110, 120, 129, and 138). Rather, they plead the facts of the President's authorization, to the exclusion of any statutory or judicial authorization, as the *essence* of the alleged activities.

Plaintiffs also argue that the Government's reading of the complaints as limited to past presidentially authorized activities ignores their request for injunctive relief to stop the alleged "*ongoing* mass surveillance." Pls.' Brief at 1; *see also id.* at 11. But Plaintiffs' requests for injunctive relief merely reflected their lack of awareness at the time that the presidentially authorized programs they contested had already ceased, not that they were challenging FISA-based programs. Indeed, Plaintiffs specifically sought an injunction prohibiting the

[14] The complaint further alleges that these written requests to telecommunications companies stated "that the Program's activities have been determined to be lawful by the Attorney General, except for one period of less than sixty days." *Id.* ¶ 43. The complaint then recounts alleged facts from March, 2004, when the Program's legality was certified by the Counsel to the President rather than the Attorney General. *Id.* ¶¶ 44-48.

Government's continued conduct of the "Program"—i.e., which the complaints defined as the acquisition of communications information pursuant to presidential authorization, not statutory or judicial authorization. *See Jewel* Compl., at Prayer for Relief (requesting an injunction "prohibiting Defendants' continued use of the Program"); *Shubert* Second Amended Compl. at Prayer for Relief (requesting a judgment enjoining "the Spying Program or any NSA electronic surveillance of United States persons without a search warrant or court order"); Plaintiff-Appellants' Ninth Circuit Opening Brief, Case No. 10-15616, at 1 (ECF No. 16) ("Plaintiffs seek . . . an injunction halting surveillance of Plaintiffs and class members under the Program").

Plaintiffs' argument that the Government failed to consult with them or notify the Court about its understanding of Plaintiffs' complaints ignores the secrecy essential to the successful conduct of classified intelligence programs, and belies the record of this litigation. Pls.' Brief at 1-2, 14-15, 18. As an initial matter, the notion that the Government should have raised its understanding of the complaints with Plaintiffs or the Court incorrectly presupposes that the Government harbored questions about the scope of Plaintiffs' claims, or had reason to do so. It did not, given that Plaintiffs' complaints clearly challenged only presidentially authorized programs. Moreover, even if the Government had been unclear about whether Plaintiffs' complaints included FISC-authorized activities, it could not have simply asked Plaintiffs for clarification because those very FISC-authorized activities and the orders that authorized them were classified state secrets at the time. Plaintiffs' blithe suggestion that the Government should have just asked them whether their claims extended to FISC-authorized activities disregards the obvious fact that to pose such a question would have effectively revealed the existence of those highly sensitive and (at the time) still classified intelligence programs.

Although it was unable to communicate with Plaintiffs on this subject without risking harmful disclosures of highly classified information, the Government did, however, inform the Court in 2007, through a classified submission, of its understanding that Plaintiffs challenged only presidentially authorized activities and the implications for the Government's preservation obligations—specifically, that it was preserving a range of documents and information concerning the presidentially authorized activities at issue in the complaints, but not information

about activities conducted pursuant to FISC orders. *See* Gov't Defs.' Opening Brief at 5-7, 19-20. The Government also offered to address any questions the Court may have had in a classified setting. *Id*. at 7.[15] At no point did the Court take issue with the Government's plainly stated understanding of the scope of the case or its preservation obligations. These notifications cannot be dismissed as "a handful of secret statements . . . referring to [the Government's] . . . reading of the complaint." Pls.' Brief at 2.

Particularly unpersuasive is Plaintiffs' continued argument that the Government acknowledged in its state secrets privilege declarations that the complaints encompass FISC-authorized activities. *Id.* at 15-17. Conspicuously absent from this argument is any rebuttal to the Government's point, now made in two briefs, that the passages from which Plaintiffs selectively quote merely explain that litigating Plaintiffs' claims about presidentially authorized activities risks disclosing sources and methods still currently employed in FISC-authorized programs. Gov't Defs.' Opening Brief at 22-24; Gov't Defs.' Resp. to Pls.' Opening Brief re: Preservation at 21-23 (ECF No. 193). That was the declarants' meaning, for example, when they said the *Hepting* complaint "'puts at issue sources and methods for surveillance activities conducted pursuant to orders of the [FISC].'" Pls.' Brief at 16 (quoting Redacted Classified Decl. of Lt. Gen. Keith B. Alexander, Director, NSA, ¶ 37 (ECF No. 224)).

Plaintiffs provide no response to this point, and instead continue to selectively quote and misconstrue the declarations. For example, Plaintiffs quote the statement in the NSA's 2012 declaration that "Plaintiffs' allegations put at issue all three NSA activities originally authorized by the President after the 9/11 attacks and later transitioned to FISA authority." Pls.' Brief at 16 (quoting Redacted Classified Decl. of Frances J. Fleisch, NSA ¶ 6 (ECF No. 172-8)). When this statement is viewed in context rather than isolation, however, its meaning becomes clear—that

[15] The Government had also previously informed the Court, in June 2006, about the retention limitations contained in the FISC's orders authorizing these intelligence activities, specifically notifying the Court about the requirement contained in the FISC order authorizing the Section 215 bulk telephony metadata program that metadata be destroyed after five years. *Id.* at 5. And the Government told the Court, in December 2013, that it had completed destruction of all Internet metadata collected under FISC authorization pursuant to the pen register and trap-and-trace provision of FISA, 50 U.S.C. § 1842. Redacted Classified Declaration of Frances J. Fleisch, NSA, at 53 n.32 (Dec. 20, 2013) (ECF No. 227).

Plaintiffs' allegations put FISC-authorized activities "at issue" only to the extent that proving that their allegations of a content dragnet are false could risk disclosure of current sources and methods of intelligence gathering. In the same vein, the statement Plaintiffs selectively quote from DNI Clapper's 2013 declaration—that further litigation would require or risk disclosure of information concerning targeted content surveillance and bulk collection activities (Pls.' Brief at 16-17)—actually begins "[i]n order to address plaintiffs' allegation that the NSA … ha[s] indiscriminately intercepted the content and obtained the communications records of millions of Americans *as part of an alleged presidentially authorized 'Program'* after 9/11 . . . ." Redacted Classified Decl. of James L. Clapper, DNI, ¶ 12 (ECF No. 220) (emphasis added). The paragraph Plaintiffs cite from the NSA's 2013 declaration (*see* Pls.' Brief at 17), also describes Plaintiffs' allegations as limited to post-9/11 presidentially authorized activities. Redacted Classified Decl. of Frances J. Fleisch, NSA ¶ 27 (ECF No. 227).

Likewise, Plaintiffs claim that the DNI "asserted that plaintiffs' allegations include the activities authorized by the FISC, specifically referencing 'current surveillance activities' and FISC orders." Pls.' Brief at 16 (quoting Redacted Classified Declaration of James R. Clapper, Director of National Intelligence, ¶ 57 (ECF No. 172-7)). But in the paragraph Plaintiffs quote, DNI Clapper merely asserted *privilege* over information concerning NSA activities conducted pursuant to FISC authority, specifying current surveillance activities; he said nothing about Plaintiffs' allegations. Plaintiffs also distort the meaning of DNI Negroponte's reference to FISC-authorized programs by juxtaposing sentences separated by wide swaths of redacted text. Pls.' Brief at 16 (quoting Redacted Classified Declaration of John D. Negroponte, Director of National Intelligence, ¶ 3 (ECF No. 222)).

In sum, Plaintiffs distort the central point of the Government's state secrets privilege declarations—that disclosing sources and methods of *past* activities challenged in these cases, where the NSA continues to rely on those sources and methods, would place current intelligence programs at risk. At the same time, they ignore the declarants' consistent reference to Plaintiffs' allegations as challenging the past activities that President Bush alone authorized after 9/11.

Apart from their misplaced reliance on their complaints and the Government's own declarations, Plaintiffs point only to passing remarks contained in just two out of the hundreds of filings made in these cases as evidence that they "notified" the Government of the true scope of their claims. The first is located in a footnote to their January 2007 opposition to a Government stay motion in the multi-district litigation. *See* Pls.' Brief at 14 (citing Opp. to Stay, *MDL* ECF No. 128 at 3-4 n.2). There Plaintiffs stated that FISC oversight of the Terrorist Surveillance Program, involving (in Plaintiffs' own words) "electronic surveillance of international communications involving al Qaeda suspects," was "irrelevant to [their] claim that … carriers are assisting the government in the interception and electronic surveillance of all or most of the communications, both domestic and international, that transit the carriers' networks." *See id.* But this statement thus tends to confirm, not refute, that Plaintiffs were challenging an alleged program of domestic mass surveillance rather than the targeting of non-U.S. persons located overseas, as conducted under Section 702. *See* Gov't Defs.' Opening Brief at 16. The second statement appeared more than three years later in Plaintiffs' appellate brief, Pls.' Brief at 15 (citing *Jewel v. NSA*, Plaintiffs-Appellees' Reply Br. at 24 n.9), where Plaintiffs remarked that "hypothetical FISC orders" authorizing the surveillance they alleged would not satisfy statutory or Fourth Amendment requirements. This statement of opinion, also submerged in a footnote in one of hundreds of filings Plaintiffs have made in these cases, cannot reasonably be portrayed as "notification" to the Government that the complaints, which speak exclusively of presidentially authorized programs, were also meant to challenge FISA-based activities.

Plaintiffs' argument that their complaints encompass intelligence activities conducted pursuant to Section 702 of the FISA is particularly specious, in light of both (1) their express statements to the contrary during this litigation; and (2) the fact that Section 702 authorizes targeted surveillance of non-U.S. persons abroad, not mass surveillance of Americans' communications. As explained in the Government's opening brief and in the Government's opposition to Plaintiffs' emergency application to enforce the TRO, Section 702 authorizes a publicly acknowledged intelligence-collection program that clearly operates pursuant to both statutory and judicial authority. It was enacted in 2008 before the *Jewel* Plaintiffs filed their

complaint, and its constitutionality was challenged in a publicly filed lawsuit the day it was enacted. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1146 (2013). Plaintiffs did not, however, challenge any Section 702 activities in their complaint, and they subsequently disclaimed any relevance of Section 702 to their claims. Gov't Defs.' Opening Brief at 16-17; Opp. to Pls.' Emergency App. to Enforce TRO at 15. Further confirmation that they knew about that provision is that the *Jewel* complaint was itself a response to a provision of the same legislation (the FISA Amendments Act of 2008) that provided immunity for the telecommunications companies that Plaintiffs had sued in *Hepting*. *See* 50 U.S.C. § 1885a.

Plaintiffs' prior admissions that Section 702 is irrelevant to their claims are consistent with their arguments that their case is about mass domestic surveillance, not targeted surveillance of non-U.S. persons. As noted above, the Section 702 program undisputedly involves 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 (and in fact prohibits intentional acquisition of any wholly domestic communications). *See supra* Section I; 50 U.S.C. §§ 1881a(a), (b); *Amnesty Int'l*, 133 S. Ct. at 1144. Indeed, Plaintiffs have repeatedly distinguished the mass surveillance they allege from Section 702 on this basis. *See, e.g.*, Jewel Plaintiffs' Supplemental Brief Re: *Clapper v. Amnesty International USA* at 1 (ECF No. 140) ("The *Clapper* plaintiffs brought a facial challenge to a newly-enacted statutory provision *not at issue here*, 50 U.S.C. § 1881a [Section 702], which authorizes surveillance targeted at foreigners outside the United States.") (emphasis added); Plaintiffs' Responses to the Court's Four Questions at 10-11 (ECF No. 177) ("*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*") (emphasis added).

Nor is any incidental collection of domestic communications that occurred (or may occur) under the NSA's upstream collection the type of dragnet surveillance of which Plaintiffs complain. As noted above, the FISC opinions discussing upstream acquisition of multiple communications transactions make clear that this collection occurs incidentally, due to technical limitations. *See, e.g.*, Oct. 3, 2011 FISC Op., 2011 WL 10945618, at *10. Nor is there any "monitor[ing]" of domestic communications as a result of this collection. *See Shubert* Plaintiffs' Brief Concerning The Gov't's Violation of The Court's Preservation Orders at 1 (*Shubert* ECF No. 124). The NSA's Section 702 program is simply not the "dragnet" acquisition of the communications of "practically every American who uses the phone system or the Internet" that Plaintiffs' allege. *Jewel* Compl. ¶ 9; *see also Shubert* 2d Am. Compl. ¶¶ 1, 2, 5.

III. PLAINTIFFS HAVE MADE NO SHOWING OF SPOLIATION THAT WOULD JUSTIFY AN ADVERSE INFERENCE, PARTICULARLY ON A QUESTION OF THE COURT'S SUBJECT MATTER JURISDICTION.

Plaintiffs not only insist that the Government should be burdened with onerous preservation requirements, concerning programs not at issue in this case, that could drastically impair the operation of NSA intelligence programs, *see* Decl. of Richard H. Ledgett, Jr., Deputy Director, NSA (ECF No. is 244) ¶¶ 2-3, 6, 8; but they also maintain that the Government spoliated evidence by complying with FISC-ordered limits on the retention of communications information collected under the statutorily based intelligence programs that they now contend are at issue. As a sanction, Plaintiffs seek an adverse "inference" that information concerning their communications has been collected under these programs. Plaintiffs have made no showing of spoliation that warrants this unjust result, and should not be relieved of their burden to establish their standing to challenge the activities at issue.

A. Plaintiffs Have Not Established a Spoliation Claim.

Plaintiffs raise claims of spoliation because the Government complied with the letter and spirit of FISC-ordered retention limits applicable to bulk telephony metadata collected between 2006 and 2009, bulk Internet metadata collected between 2006 and 2011, and upstream data collected between 2007 and 2012. Pls.' Brief at 8. Spoliation cannot occur, however, where there is no underlying duty to preserve. *See Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d

976, 989 (N.D. Cal. 2012) ("*Apple II*"). "The scope of the duty to preserve extends to what the party knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request." *Keithley v. Homestore.com, Inc.*, 2008 WL 4830752, at *7 (N.D. Cal. Nov. 6, 2008); *see also Apple, Inc. v. Samsung Elecs., Co.*, 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012) ("*Apple I*") (obligation to preserve extends to information that is "relevant to specific, predictable, and identifiable litigation"). Even where the duty to preserve exists, "[t]he bare fact that evidence has been altered or destroyed does not necessarily mean that the party has engaged in sanction-worthy spoliation," *Reinsdorf v. Skechers U.S.A., Inc.*, 296 F.R.D. 604, 626 (C.D. Cal. 2006), because "a party should only be penalized for destroying documents if it was wrong to do so" under the circumstances. *Akiona v. United States*, 938 F.2d 158, 161 (9th Cir. 1991). *See, e.g., United States v. Kitsap Phys. Serv.*, 314 F.3d 995, 1001 (9th Cir. 2002) (rejecting spoliation argument where, *inter alia*, defendants "offered credible reasons for the destruction of the records").

In order to prove spoliation, "a party must show: (1) the party with control over the evidence had an obligation to preserve it at the time of destruction; (2) the evidence was destroyed with a 'culpable state of mind'; and the evidence was relevant to the party's claim or defense." *Domingo v. Donahoe*, 2013 WL 40400913, at *4 (N.D. Cal. Aug. 7, 2013); *accord Apple II*, 888 F. Supp. 2d at 989–90; *Toppan Photomasks, Inc. v. Park*, 2014 WL 2567914 at *4 (N.D. Cal. May 29, 2014). "The party seeking spoliation sanctions has the burden of establishing the elements of a spoliation claim." *Reinsdorf*, 296 F.R.D. at 626. Plaintiffs have entirely failed to carry this burden.

1. Plaintiffs have not shown that the Government had a duty to preserve information acquired under FISC authority.

First, Plaintiffs have failed to establish that the Government had a duty to preserve information concerning FISC-authorized activities, *see Domingo*, 2013 WL 4040091 at *4, for all the reasons stated above and in the Government's previous filings on this subject. *See supra* Section II; Gov't Defs.' Response to Pls.' Opening Br. re: Evid. Preservation (ECF No. 193) at

15–34; *see also* Gov't Defs.' Opening Brief at 13-26. The *Jewel* and *Shubert* complaints—notwithstanding Plaintiffs' wholesale attempt to rewrite them—are clearly directed at presidentially authorized NSA intelligence activities, unauthorized by statute or court order, following the terrorist attacks of 9/11. *See id*. Despite numerous opportunities to do so, Plaintiffs have failed to explain how claims taking issue with specified intelligence programs precisely because they were presidentially, not judicially, authorized can be taken now to encompass FISC-authorized programs, or, by the same token, why the Government's preservation duties should be construed as extending to those programs. Because this threshold element has not been satisfied, there can be no finding of spoliation.

2. Plaintiffs have failed to establish that the Government Defendants possessed the requisite state of mind for a finding of spoliation.

Even assuming the Government had a duty to preserve intelligence information acquired under FISC authority in these cases, Plaintiffs have failed to "establish . . . that the records were destroyed 'with a culpable state of mind.'" *Apple II*, 888 F. Supp. 2d at 989 (quoting *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002)). "A party's destruction of evidence qualifies as willful spoliation if the party has some notice that the documents were potentially relevant to the litigation before they were destroyed," *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 959 (9th Cir. 2006), but not where a party without such notice "merely destroys evidence pursuant to a document retention policy." *Pirv v. Glock, Inc.*, 2009 WL 54466, at *5 (D. Or. Jan. 8, 2009) (quoting *Akiona*, 928 F.2d at 161); *Brock v. Cnty of Napa*, 2012 WL 2906593, at *6 (N.D. Cal.) (same).

As explained above and in the Government's previous briefs on this matter, nothing in the complaints, or in any of Plaintiffs' subsequent filings, provided the Government with reasonable notice that they were challenging activities undertaken pursuant to judicial orders issued under FISA, including the FISC-authorized Section 215 telephony metadata program or (discontinued) bulk Internet metadata program. *See supra* Section II; *see also* Gov't Defs.' Opening Brief at 13-26. This is particularly so regarding Section 702, which involves targeted surveillance of non-U.S. persons, bears no resemblance to Plaintiffs' allegations about "dragnet"

surveillance of communications content, and which Plaintiffs have consistently dismissed as irrelevant to their claims. *See supra* at 17.

There is no basis whatsoever to conclude that this case involves the willful destruction of documents a party knows to be relevant to the lawsuit—the scenario in most spoliation cases. To the contrary, the Government has based its preservation efforts on the facts alleged in Plaintiffs' complaints, and otherwise has complied with the FISC-mandated retention limits applicable to programs that do not fall within the scope of these cases. As discussed *supra*, Section I, these retention limits are integral to the lawful operation of the programs in compliance with statutory requirements, and, as found by the FISC, rights protected by the Fourth Amendment. Thus, far from "conscious disregard" of a legal obligation to preserve evidence, *Apple II*, 888 F. Supp. 2d at 998, the Government acted to comply with the only applicable legal duty of which it had been made aware—an irreproachable objective. *See, e.g.*, *Kitsap Physicians Serv.*, 314 F.3d at 1001 (rejecting spoliation argument where, *inter alia*, defendants "offered credible reasons for the destruction of the records, i.e., the [six-year] retention policy in accordance with both State and Federal Regulations"); *Med. Lab. Mgmt. v. American Broad Co.*, 306 F.3d 806, 824 (9th Cir. 2002) (rejecting sanctions for spoliation where party's non-retention of documents was due to "an innocent reason"); *Akiona*, 938 F.2d at 161 (similar; regarding government's adherence to two-year destruction policy); *see also, e.g.*, *Bull v. UPS, Inc.*, 665 F.3d 68, 79 (3d Cir. 2012) (spoliation not sanctionable "*where the failure to produce [document or information] is otherwise properly accounted for*"); *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (same). For their part, Plaintiffs cite no authority for the unstated proposition that underlies their position, that spoliation may be found where a party has done nothing more than comply with orders of a coordinate Article III court having jurisdiction over the matter in question (specifically, jurisdiction conferred by Congress to ensure the lawful conduct of FISA-based surveillance programs), particularly where the Government rightly believed that those matters were not the subject of litigation. Thus, Plaintiffs have also failed to meet their burden with respect to the second prong of the spoliation test.

B. Plaintiffs Cannot Confer Subject Matter Jurisdiction on the Court by Means of an Extreme and Unwarranted Adverse Inference Sanction.

Even assuming for the sake of argument that preservation of evidence regarding FISC-authorized programs were required here (which, for the reasons stated above, it is not), the sanction sought by Plaintiffs would remain wholly unwarranted. The present situation involves several years' worth of communications data, acquired in the course of FISC-authorized intelligence programs, that lack relevance to the presidentially authorized activities challenged by the complaints. The data were discarded for the undisputed purpose of complying with requirements imposed by an Article III court that it determined were necessary to protect the privacy of U.S. persons, and ensure the programs' constitutionality. The NSA continues to maintain repositories of the very same types of data that are not (or are not yet) subject to destruction under these FISC-imposed retention limits. Thus, in all events, the extreme sanction sought by Plaintiffs of an "adverse inference"—in truth, and adverse finding of fact—"that their communications and communications records were collected by the government as part of the mass surveillance programs at issue," Pls.' Brief at 20, is neither justifiable nor reconcilable with this Court's independent obligation to assure itself of its jurisdiction, and not presume it.

The penalty for spoliation "can range from minor sanctions, such as the awarding of attorneys' fees, to more serious sanctions, such as . . . instructing the jury that it may draw an adverse inference," *Apple I*, 881 F. Supp. 2d at 1135; *see also Apple II*, 888 F. Supp. 2d at 989, usually meaning an inference "that the spoiled or destroyed evidence would have been unfavorable to the responsible party." *Med. Lab. Mgmt.*, 306 F.3d at 823-24; *see also Ingrid & Isabel LLC v. Baby Be Mine LLC*, 2014 WL 1338480, at *7 (N.D. Cal. Apr. 1, 2014). The judges of this Court have consistently recognized that "[a]n adverse inference sanction is an extreme sanction that should not be given lightly." *Toppan Photomasks*, 2014 WL 2567914, at *10 (internal quotation marks and citation omitted); *SEC v. Mercury Interactive, LLC*, 2012 WL 3277165, at *10 (N.D. Cal. Aug. 9, 2012); *Ahcom, Ltd. v. Smeding*, 2011 WL 3443499, at *8 (N.D. Cal. Aug. 8, 2011) (referring to adverse inference as a "severe sanction"); *Keithley*, 2008 WL 4830752, at *10 ("a harsh remedy").

In cases involving spoliation, this Court has applied a three-factor test to determine whether an adverse inference (or other sanction) is appropriate: "(1) the degree of fault of the party who destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether a lesser sanction would avoid substantial unfairness to the opposing party." *E.g., Toppan Photomasks*, 2014 WL 2567914 at *8. Thus, while a finding of bad faith is not a prerequisite to an adverse inference sanction, *Glover v. BIC Corp.*, 6 F.3d 1318, 1329 (9th Cir. 1993), "'a party's motive or degree of fault in destroying evidence is relevant to what sanction, if any, is imposed.'" *Toppan Photomasks*, 2014 WL 2567914, at *8 (quoting *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1066-67 (N.D. Cal. 2006). Similarly, where the opposing party suffers little or no prejudice from loss of the destroyed evidence, this Court has refused adverse inference sanctions. *See Toppan Photomasks*, 2014 WL 2567914 at *10; *PersonalWeb Techs., LLC v. Google, Inc.*, 2014 WL 580290, at *4 (N.D. Cal. Feb. 13, 2014); *Ahcom*, 2011 WL 3443499, at *8, *9; *Mercury Interactive*, 2012 WL 3277165 at *11; *Hamilton v. Signature Flight Support Corp*., 2005 WL 3481423 at *3 (N.D. Cal. Dec. 20, 2005).

An adverse inference sanction, moreover, "'can take many forms … ranging in degrees of harshness,'" *Apple II*, 888 F. Supp. 2d at 994 (quoting *Apple I*, 881 F. Supp. 2d at 1150), from allowing the trier of fact to decide whether a party's failure to preserve evidence is important to the outcome of the case, *e.g., Jackson Family Wines v. Diageo N. Am., Inc.*, 2014 WL 595912, at *8 (N.D. Cal. Feb. 14, 2014), to establishment of a rebuttable presumption, *e.g., IO Group, Inc., v. GLBT Ltd.*, 2011 WL 4974337, at *8 (N.D. Cal Oct. 19, 2011), to permitting the trier of fact to find the offending party's destruction of evidence "determinative" of issues in the case, *Apple II*, 888 F. Supp. 2d at 994-95. The nature and scope of the adverse inference granted, like the choice of a spoliation sanction generally, must also be determined in light of the degree of the responsible party's fault and the level of prejudice suffered by the opponent. *See id.* at 999. Notably, the adverse "inference" sought by Plaintiffs here lies at the extreme end of the spectrum—not so much an inference, allowing the trier of fact to infer that the destroyed data would have been harmful to the Government's case, or even a presumption, but an irrebuttable conclusion that information about Plaintiffs' communications was collected by the Government

as part of the intelligence programs that Plaintiffs now maintain are at issue in these cases. Pls.' Brief at 20. Plaintiffs cite no precedent in which this Court has administered such an extreme sanction in circumstances such as those presented here. Nor should it do so in this instance.

1. The Government cannot be faulted for complying with retention limits imposed by FISC orders.

Plaintiffs' claims of spoliation involve three sets of data: (1) "upstream" communications data collected under authority of Section 702 (and a precursor statute) between 2007 and 2012; (2) bulk telephony metadata collected under Section 215 of the USA Patriot Act, 50 U.S.C. § 1861, between 2006 and 2009; and (3) bulk Internet metadata collected under the pen register and trap-and-trace provision of FISA, 50 U.S.C. § 1842, between 2006 and 2011. Pls.' Brief at 8; *see generally* Classified Declaration of Teresa H. Shea (unclassified public version) (ECF No. 228) ("Classified Shea Decl.") ¶¶ 33, 34, 37-38.

As explained above, yet nowhere acknowledged by the Plaintiffs, the NSA destroyed upstream communications information collected under Section 702—without any reasonable basis to believe that Section 702 was at issue in these lawsuits—for the undisputed purpose of complying with the express retention limits set forth in minimization procedures mandated by the statute, and the FISC, in order to protect the privacy interests of U.S. persons and meet Fourth Amendment standards. *See supra* Section I; 50 U.S.C. § 1881a(c)(1)(A), (e)(2), (i)(2)(C), (3); Classified Shea Decl. ¶¶ 37-38. Similarly, the NSA destroyed bulk telephony metadata acquired between 2006 and 2009—without any reasonable basis to believe that the Section 215 program was at issue in these lawsuits—to comply with the terms of FISC orders which, pursuant to the mandate of Section 215 to impose minimization requirements to protect the privacy interests of U.S. persons, compel the Government to destroy such data within five years of collection. 50 U.S.C. § 1861(c)(1), (g)(2)(A); *First Unitarian Church of Los Angeles v. NSA*, No. 13-cv-3287-JSW, ECF No. 67-7 (Declaration of Teresa H. Shea, Signals Intelligence Director, NSA) ¶ 30; *id.* Exh. A (Primary Order) at 14; *see* Classified Shea Decl. ¶ 33. Likewise, following the termination of the bulk Internet metadata program in December 2011, the Government destroyed the metadata accumulated under that program, as a matter of prudence

consistent with the spirit of the governing FISC orders that also limited retention of those data to five years after collection. Classified Shea Decl. ¶ 34; *see First Unitarian*, ECF No. 67-17 (*[Redacted]*, Dkt. No. PR/TT [redacted], Opinion and Order (F.I.S.C. [redacted]) (declassified and released on Nov. 18, 2013)) at 71. No litigant should be sanctioned as a "spoliator" for complying with lawful court orders, especially where, as here, it had no substantial reason to believe that the destroyed records were pertinent to its opponents' claims. *Ingrid & Isabel LLC*, 2014 WL 1338480, at *7 (spoliation sanctions 'should be commensurate to the spoliating party's motive or degree of fault"); *Jackson Family Wines*, 2014 WL 595913, at *6 (same); *see also Med. Lab. Mgmt.*, 306 F.3d at 824 (where evidence is lost "for an innocent reason" an adverse inference sanction may be rejected); *Akiona*, 938 F.2d at 161 (rationale for drawing an adverse does not apply where destruction of the records does not suggest they would have been threatening to the defense of the case).[16]

Plaintiffs nevertheless seek to assign fault to the Government on the asserted grounds that its interpretation of their complaints is not reasonable, and that it ignored opportunities to clarify the scope of their claims and its corresponding preservation duties with their counsel and the courts even after they (allegedly) disputed the Government's reading of their complaints. Pls.' Brief at 21; *see id.* at 18. None of these arguments can be squared with reality. Notwithstanding Plaintiffs' labored efforts to re-write the history of this litigation, neither the objective terms of their complaints, nor any statements made in their subsequent filings, gave the Government any substantial reason to believe that their claims encompassed these programs. Contrary to their baseless assertion that the Government ignored its duty of candor to this Court and the FISC, *id.* at 18, 21, the Government made clear to the Court in 2007 that it construed the Plaintiffs' claims

[16] This is all the more so considering the repositories of the same categories of data that the NSA continues to retain, a fact that Plaintiffs also fail to acknowledge. The NSA continues to retain all of the telephony metadata, Internet metadata, and communications content collected under the President's Surveillance Program. Redacted Classified Decl. of Miriam P., NSA (ECF No. 230) ¶¶ 36, 38, 39. As permitted by the FISC's orders, the Government also currently retains bulk telephony metadata collected under authority of Section 215 between 2009 and the present, and upstream data collected between 2012 and the present. Classified Shea Decl. ¶¶ 33, 38. The retention of these data underscores the indisputable fact that the Government's destruction of data was motivated by its legal obligation under FISA, and the FISC's orders, and had nothing to do with Plaintiffs' claims.

and its corresponding preservation obligations as solely encompassing presidentially authorized activities; invited queries from the Court on the matter; and, receiving none, had no reason to believe that it was subject to "potentially conflicting" legal duties that it needed to raise with this Court or the FISC. In contrast it is Plaintiffs who, even after the public transition of the Terrorist Surveillance Program to FISC oversight in January 2007, failed to articulate in their complaints the legal challenges to FISC-authorized intelligence programs that they now insist they always meant to bring.

2. Plaintiffs have suffered no prejudice that justifies an adverse inference sanction.

Plaintiffs have also failed to make the necessary showing of prejudice to obtain an adverse inference. The prejudice inquiry looks to "whether the spoiling party's actions impaired the non-spoiling party's ability to go to trial or threatened to interfere with the rightful decision of the case." *Toppan Photomasks*, 2014 WL 2567914 at *9; *Ingrid & Isabel LLC*, 2014 WL 1228480 at *7. Plaintiffs' circular argument that they have been prejudiced by the destruction of the data because the data have been destroyed, Pls.' Brief at 21, overlooks that the Government continues to preserve or maintain for intelligence purposes (so far as permitted by FISC orders) many years' worth of bulk telephony metadata, bulk Internet metadata, and intercepted communications that could, in theory, be examined to ascertain whether the contents of or metadata pertaining to Plaintiffs' telephonic or on-line communications have been collected. This Court has often declined to impose adverse inference sanctions where the availability of alternative sources of evidence promised to mitigate the risk of prejudice to a spoiling party's opponent. *Toppan Photomasks*, 2014 WL 2567914 at *9-10 (citing precedents); *Apple II*, 888 F. Supp. 2d at 994-95; *Ahcom*, 2011 WL 3443499, at *8-9 (citing *Med. Lab. Mgmt.*, 306 F.3d at 825); *Keithley*, 2008 WL 4830752, at *10; *Gippetti v. UPS, Inc.*, 2008 WL 3264482, at *4 (N.D. Cal. Aug. 6, 2008) (Lloyd, M.J.); *Hamilton*, 2005 WL 3481423, at *8. That is also the situation here, and provides yet an additional reason why no adverse inference sanction is warranted.[17]

[17] Reinforcing that conclusion is the fact that the discarded data were subject to the Government's assertion of the state secrets privilege over documents and information that would tend to confirm or deny the identities of targets or subjects of NSA intelligence-gathering activities, or of the telecommunications service providers that participate in those activities.

3. A federal court may not presume its Article III jurisdiction as a spoliation sanction.

Because the Government cannot be faulted for its reasonable interpretation of Plaintiffs' complaints, or for complying with lawful orders of the FISC, and Plaintiffs have shown no prejudice, there is no basis here to award even the weakest of adverse inferences. *See Apple II*, 888 F. Supp. 2d at 993. Plaintiffs' request must also be denied, however, for the additional reason that the "inference" they seek is impermissible, as it asks this Court to conclusively presume its subject-matter jurisdiction under Article III.

As the Government has discussed in numerous prior briefs, proof that information concerning Plaintiffs' communications has been subject to collection under the intelligence programs they purport to challenge is necessary to demonstrate their standing, which is itself essential to establishing the presence of an Article III case or controversy. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). By requesting an adverse inference that information pertaining to their communications has been collected under all of the "mass surveillance programs at issue," Pls.' Brief at 20 (including a mass content "dragnet" that has never existed), Plaintiffs ask this Court to presume its Article III jurisdiction as a sanction for alleged spoliation, based on "Rule 37 and the court's inherent power." Pls.' Brief at 19. A federal court, however, "has an obligation to assure itself of its jurisdiction before proceeding to the merits." *Atalig v. United States*, 554 F. App'x 662, 663 (9th Cir. 2014). Jurisdiction must "appear[ ] affirmatively from the record" and cannot be presumed. *Table Bluff Reservation (Wiyot Tribe) v. Philip Morris Inc.*, 256 F.3d 879, 882 (9th Cir. 2001).

Alleged discovery misconduct cannot create subject-matter jurisdiction where none exists. As to Rule 37, the Federal Rules of Civil Procedure "do not extend or limit the

---

Public Declaration of James R. Clapper, Director of National Intelligence (Dec. 20, 2013) (ECF No. 168) ¶¶ 2, 10, 19. As a result of the Government's valid assertion of privilege, *see Jewel v. NSA*, 965 F. Supp. 2d 1090, 1103 (N.D. Cal. 2013), those data would have been removed from the case and unavailable for purposes of litigating Plaintiffs' claims. *See id.* at 1101-02 (citing *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998)). That is yet further reason why Plaintiffs cannot in any practical sense claim prejudice from the data's loss. Moreover, even if the lost data would have been available for *ex parte, in camera* consideration by the Court under 50 U.S.C. § 1806(f), *see Jewel*, 965 F. Supp. 2d at 1103-06 (a proposition with which the Government respectfully continues to disagree), the same would be true of the data the NSA still possesses, again defeating any claim of ascertainable prejudice.

jurisdiction of the district courts." Fed. R. Civ. P. 82. Nor is a district court's inherent power to sanction discovery misconduct a source of subject-matter jurisdiction. *See A-Z Int'l v. Philips*, 323 F.3d 1141, 1145 n.2 (9th Cir. 2003) (citing *Chambers v. NASCO, Inc.*, 501 U.S. 32, 43 (1991) ("the district court may not exercise subject-matter jurisdiction in this cause solely on the basis of [the plaintiff's] invocation of the court's power to sanction contempt."). Indeed, the Supreme Court has recognized that "no action of the parties can confer subject-matter jurisdiction upon a federal court." *Insurance Corp. of Ireland v. Compagnie des Bauxites de Guinee*, 456 U.S. 694, 702 (1982).

In *Insurance Corp. of Ireland*, the Supreme Court held that *personal* jurisdiction could be established through an adverse inference under Rule 37(b)(2)(A), but the Court emphasized that it was possible to do so because personal jurisdiction—unlike subject matter jurisdiction—"represents first of all an individual right" that "like other such rights [can] be waived." 456 U.S. at 703. There, the defendants argued that an adverse inference could not be used to establish jurisdictional facts because "it is impermissible to use a fiction to establish judicial power, where, as a matter of fact, it does not exist." *Id.* at 701. The Court rejected this argument as to personal jurisdiction, observing that "this represents a fundamental misunderstanding of the nature of personal jurisdiction." *Id.* The Court explained that the defendants "fail[ed] to recognize the distinction between the two concepts [of subject-matter jurisdiction and personal jurisdiction]," and highlighted that "their argument's strength comes from conceiving of jurisdiction only as subject-matter jurisdiction." *Id.* The Court then went on to describe, at length, the function of subject-matter jurisdiction as a limit on the federal courts' power, and emphasized the "legal consequences [that] directly follow from this," including that, as to subject matter jurisdiction, "the consent of the parties is irrelevant, . . . principles of estoppel do not apply, . . . and a party does not waive the requirement by failing to challenge jurisdiction early in the proceedings." *Id.* at 702 (internal citations omitted).

Thus, in holding that an adverse inference could be used to establish personal jurisdiction, the Supreme Court implied that the same could not be done for subject-matter jurisdiction. *Id.* at 701; *cf. Grupo Dataflux v. Atlas Global, L.P.*, 541 U.S. 567, 576 (2004) ("a

court's subject-matter jurisdiction cannot be expanded to account for the parties' litigation conduct"). Indeed, subsequently, in *Steel Co. v. Citizens for Better Environment*, 523 U.S. 83 (1998), the Court rejected the use of a legal fiction—"hypothetical jurisdiction"—by which lower courts in certain circumstances had "assum[ed] jurisdiction for the purpose of deciding the merits." *Id.* at 94.

The Court of Appeals in *Gibson v. Chrysler Corp.*, 261 F.3d 927 (9th Cir. 2001), citing *Insurance Corp. of Ireland*, concluded that if a discovery sanction may be employed to establish personal jurisdiction, "we see no reason why a court cannot . . . sanction a defendant who refuses to respond to appropriate discovery requests on a fact relevant to subject matter jurisdiction by entering an order establishing the facts as true." *Id.* at 948. But the Court in *Gibson*, while relying on the Supreme Court's holding as to personal jurisdiction, did not address the Supreme Court's much different discussion of subject-matter jurisdiction. *See id.* In any event, *Gibson* has no application to this case.

In *Gibson*, the Court of Appeals approved an adverse inference as a sanction for a defendant's "refus[al] to respond to appropriate discovery requests on a fact relevant to subject matter jurisdiction." *Id.* In that setting, the Court emphasized that "a sanction in the form of an adverse factual finding . . . rests on the reasonable assumption that the party resisting discovery is doing so because the information sought is unfavorable to its interest. In such a case, the sanction merely serves as a mechanism for establishing facts that are being improperly hidden by the party resisting discovery." *Id.* Thus, the result in *Gibson* rested on the Court's assessment that the defendant's resistance to discovery was indicative that the information withheld would establish that subject-matter jurisdiction actually existed.

Here, by contrast, the conduct at issue here is not resistance to a discovery request but the Government's compliance with court-ordered retention limits, mandated by the FISC to protect privacy interests and ensure the constitutionality of the Government's intelligence-gathering activities. *See supra* Section I. In this context—where a litigant simply obeys lawful court orders, without any reasonable notice of an asserted legal obligation to preserve the information in question—there can be no inference as in *Gibson* that the conduct of which Plaintiffs

complain shows that evidence of subject-matter jurisdiction actually existed. Thus, by seeking an adverse inference on subject-matter jurisdiction here, Plaintiffs are asking the Court "to use a fiction to establish judicial power" where they have not shown as a matter of fact that it exists. *Insurance Corp. of Ireland*, 456 U.S. at 701. For this and all of the reasons explained above, that request should be rejected.

CONCLUSION

For the foregoing reasons, as well as the reasons set forth in the Government Defendants' opening brief, the Government has complied with the preservation orders in *Jewel* and *Shubert*, and Plaintiffs' request for spoliation sanctions should be denied.

Dated: June 27, 2014

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
BRYAN DEARINGER
Trial Attorney
bryan.dearinger@usdoj.gov
RODNEY PATTON
Trial Attorney
rodney.patton@usdoj.gov
JULIA BERMAN
julia.berman@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470

Attorneys for the Government Defendants
Sued in their Official Capacities