

***Jewel v. NSA*, No. 08-cv-4373-JSW, Joint Letter Brief re Discovery Dispute**

Richard R. Wiebe (SBN 121156)  
wiebe@pacbell.net  
LAW OFFICE OF RICHARD R. WIEBE  
One California Street, Suite 900  
San Francisco, CA 94111  
Telephone: (415) 433-3200  
Fax: (415) 433-6382

[Additional counsel on signature page.]

Counsel for Plaintiffs

James J. Gilligan  
Special Litigation Counsel  
james.gilligan@usdoj.gov  
U.S. DEPARTMENT OF JUSTICE, CIVIL  
DIVISION  
20 Massachusetts Avenue, NW, Rm. 6102  
Washington, D.C. 20001  
Telephone: (202) 514-3358  
Fax: (202) 616-8470

[Additional counsel on signature page.]

Counsel for the Government Defendants

Pursuant to the Court's Civil Standing Orders, plaintiffs Jewel, Hepting, Hicks, Knutzen, and Walton and Government Defendants National Security Agency, Department of Justice, and the United States hereby submit the following joint letter brief setting forth their respective positions on disputed discovery issues.

**Plaintiffs' Statement:**

The Court has ordered that discovery go forward on plaintiffs' Wiretap Act and Stored Communications Act ("SCA") claims (Counts 9, 12, 15). ECF No. 340. The Court's determination was based on its prior holdings that plaintiffs' statutory claims are actionable under 18 U.S.C. § 2712 and that in section 2712(b)(4) Congress preempted the state secrets privilege with respect to plaintiffs' statutory claims, substituting instead the procedure of 50 U.S.C. § 1806(f) ("section 1806(f)"). ECF No. 153 at 13, 18. The Court's order was also based on the "explicit admonition from the Ninth Circuit Court of Appeals to advance this matter." ECF No. 340 at 2.

Plaintiffs have served requests for admission, interrogatories, and document requests on the government defendants. (Plaintiffs' discovery requests are summarized in Appendix A hereto.) In their responses, the government defendants have refused to provide, either to plaintiffs or to the Court pursuant to section 1806(f), *any* new information that they have not previously publicly disclosed. The government makes three principal objections that cut through their responses: state secrets privilege; relevance objections based on the government's unilateral interpretations of the Wiretap Act and the SCA; and relevance objections based on the government's attempt to limit the temporal scope of the complaint to the pre-2007 President's Surveillance Program ("PSP"). The parties have met and conferred, but the government's position remains unchanged. Plaintiffs request that the Court overrule the objections and direct the government to respond substantively to the discovery.

**1. State Secrets Objections.** The government's principal objection to almost all of plaintiffs' discovery requests is the state secrets privilege. But the Court has already ruled—twice—that Congress preempted the state secrets privilege in section 2712(b)(4) and made the procedures of section 1806(f) the "exclusive means" governing national security evidence in statutory claims brought under section 2712. ECF No. 340 at 2-4; No. 153 at 2, 12-15. The Court has ruled that if a discovery response calls for state secret information, the government must follow section 1806(f) and make full disclosure to the Court *ex parte* for *in camera* review. ECF No. 340 at 3-4. The government never moved to reconsider those rulings, and they are law of the case.

Congress's command that the procedures of section 1806(f) are the "exclusive means" for handling national security evidence in section 2712 cases like this one and that section 1806(f) applies "[n]otwithstanding any other provision of law" also preempts the two statutory secrecy privileges (50 U.S.C. §§ 3024(i)(1), 3605(a)) the government has asserted.<sup>1</sup> 18 U.S.C. § 2712(b)(4).

The government's attempt to endlessly relitigate the state secrets issue it has twice lost must

---

<sup>1</sup> The government asserted both statutory privileges in its 2009 state secrets motion to dismiss. ECF No. 18 at 16 n.14. In its renewed state secrets motion in 2012, it chose to assert only the 50 U.S.C. § 3024(i)(1) statutory privilege (at that time, codified as 50 U.S.C. § 403-1(i)(1)), thereby waiving the 50 U.S.C. § 3605(a) privilege. ECF No. 104 at ¶ 10. By denying the government's motion, the Court necessarily rejected the 50 U.S.C. § 3024(i)(1) privilege. ECF No. 153. In any event, both privileges were enacted *before* the enactment of section 2712(b)(4) preempting prior law, including 50 U.S.C. §§ 3024(i)(1), 3605(a). Likewise, the decision in *Linder v. NSA*, 94 F.3d 693 (D.C. Cir. 1996), the government invokes is pre-section 2712 and has no bearing here.

come to an end.<sup>2</sup> Plaintiffs request that the Court overrule the government's state secrets privilege objection and related statutory objections and direct pursuant to section 1806(f) that, for each discovery response whose disclosure the government contends would harm the national security, (a) the Attorney General certify under oath separately for each discovery response that disclosure of the response would harm the national security and (b) the government prepare its substantive response and deliver the response to a court security officer who shall maintain secure custody of the response until the Court performs its *in camera* review of the response.

**2. Relevance Objections Based On The Government's Statutory Interpretations.** Under Rule 26, relevance is broadly construed and encompasses any matter relevant to the plaintiff's claims. The government has objected to numerous discovery requests for information on its mass copying and searching of communications and its acquisition of communications records on the ground that the information is not relevant to the *government's* interpretation of what conduct violates the Wiretap Act and the SCA. But that is not the standard of relevance. The standard is whether the information is relevant to the claim framed by the plaintiff, which includes the facts that the plaintiff contends are sufficient to establish her claim under her view of the governing law. *U.S. v. Real Property Located at 2366 San Pablo Ave.*, 2014 WL 2126912, at \*2-\*3 (N.D. Cal. May 22, 2014) (defendant "entitled to discovery that is relevant to its affirmative defenses, regardless of whether the Government believes these defenses have merit"; defendant's "ability to prove its defenses is not the standard against which relevance is determined").

Discovery is not the proper arena for hashing out disputed interpretations of the substantive law. That is what motions to dismiss and summary judgment motions are for. It is improper for a defendant to resist discovery on the ground that under its view of the law the information the plaintiff seeks is insufficient to prove an element of the plaintiff's claim. Notably, despite the repeated motions to dismiss and for summary judgment that defendants have brought, they have never contended that plaintiffs fail to state a claim under the Wiretap Act and the SCA.

In any event, under established law the discovery requests are relevant to plaintiffs' claims:

**a. The Wiretap Act.** The Wiretap Act prohibits the interception of electronic communications and the use or disclosure of unlawfully intercepted communications. 18 U.S.C. § 2511, subds. (1)(a), (1)(c), (1)(d). An "interception" is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

Under these provisions, the government's copying of plaintiffs' communications is an unlawful interception, and its searches of those communications are a "use." "[A]cquisition occurs 'when the contents of a wire communication are captured or redirected in any way.'" *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009); *accord U.S. v. Szymuszkiewicz*, 622 F.3d 701, 704-705 (7th Cir. 2010) (unlawful interception occurred where computer server surreptitiously made two copies of each email and sent one copy to the defendant; "The copying *at the server* was the unlawful interception, catching the message 'in flight'" (at 704; italics original)); *In re Pharmatrak, Inc.*,

---

<sup>2</sup> The government contends meritlessly that the Court has been inconsistent in its state secrets rulings and overruled its 2013 state secrets order in its 2015 Fourth Amendment order. Section 2712(b)(4), however, applies only to plaintiffs' statutory claims, not to constitutional claims.

329 F.3d 9, 22 (1st Cir. 2003) (“automatic routing program” “that automatically duplicated part of the communications . . . and sent this information to a third party” was an interception); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994) (“The recording of a telephone conversation alone constitutes an ‘aural . . . acquisition’ of that conversation.”); *In re State Police Litigation*, 888 F.Supp. 1235, 1264-65 (D. Conn. 1995) (recording telephone conversations is an interception even without listening); *George v. Carusone*, 849 F.Supp. 159, 163 (D. Conn. 1994) (same). Discovery relating to copying is thus relevant.

The government’s argument that copying is not an acquisition simply ignores the controlling authority of *Noel*. The government relies on a portion of *Sanders* holding that the transmission of oral conversations from one room to another where they were neither recorded nor listened to was not an acquisition, but ignores *Sanders*’s separate holding, quoted above, that *recording* a communication is an acquisition.

The government’s searches are a “use” of the intercepted communications. 18 U.S.C. § 2511(1)(c). By searching the communications, the government discovers whether or not they contain any selectors. Discovery related to the government’s searches is therefore relevant.

**b. SCA.** The government objects to discovery relating to communications records it obtained during the PSP on the ground that the disclosures were voluntary and not SCA violations. This objection is both legally and factually meritless. Legally, “governmental entities can be liable under § 2703(c) for soliciting information from an ISP without complying with the legal processes specified in the statute.” *Freedman v. Am. Online, Inc.*, 303 F.Supp.2d 121, 126 (D. Conn. 2004). Factually, the government did compel telecommunications providers to disclose communication records during the PSP. ECF No. 147, Ex. A at 31-32 (letter from NSA director stated assistance was “required”; letters from Attorney General “directed” compliance and said it was “required”).

Additionally, even if AT&T’s disclosure of records was voluntary and the government’s action were not a breach of its SCA duties, plaintiffs have alleged that the government is secondarily liable for aiding and abetting AT&T in violating AT&T’s duties under the SCA. Compl. ¶¶ 82-97, 253. The discovery requests are unquestionably relevant under this alternate theory of liability.

**c. Evidence of Mass Surveillance is Relevant.** Moreover, plaintiffs are entitled to discovery of the facts and circumstances surrounding the interception and searching of their Internet communications and the acquisition of their communications records. The government objects to any discovery extending beyond the communications and records of plaintiffs themselves. This information plaintiffs seek is relevant for three reasons. First, because of the mass, indiscriminate nature of its surveillance, the government may lack direct evidence of whether plaintiffs’ own communications were intercepted or searched or whether plaintiffs’ own records were acquired. Thus, it is likely that plaintiffs will need to build their case with circumstantial evidence showing they are within the class of persons whose communications and records were surveilled. Second, evidence of the government’s mass surveillance activities is relevant to the government’s intent. Third, when a plaintiff is harmed by actions the defendant has taken generally toward a class of similarly situated persons, discovery of the defendant’s actions towards the class as a whole is relevant, not just those actions that apply uniquely to the plaintiff.

Plaintiffs request that the Court overrule the government's relevancy objections to discovery requests relating to the government's copying and searching of communications and its acquisition of communications records.

**3. Temporal Scope-of-the-Complaint Objections.** The government objects to all of plaintiffs' discovery requests that touch on any events occurring after the conclusion of the PSP. This is another issue it has previously litigated and lost, and that is not the proper basis of an objection.

During the evidence preservation proceedings in 2014, the government revealed that it interpreted plaintiffs' complaint as limited to pre-2007 activities conducted under the PSP, all of which had ended before plaintiffs filed their complaint in 2008. Plaintiffs explained why the government's position was wrong (among other things, it would have meant that plaintiffs' Fourth Amendment and other injunctive relief claims were moot on their face). ECF No. 233 at 10-18; No. 260 at 2-9.

In the Fourth Amendment summary judgment proceedings challenging the current Upstream surveillance activities, the government again asserted that post-PSP conduct is outside the scope of the complaint, and asked the Court to address its cross-motion for summary judgment only if the Court concluded that post-PSP conduct is within the scope of the complaint. ECF No. 285 at 12-13 & n.3. By granting judgment in favor of the government on the Fourth Amendment Upstream issue, the Court necessarily found that Upstream and other post-PSP conduct are within the scope of the complaint. A judgment cannot be granted on a claim not put in issue by the plaintiff's complaint.

Now, having obtained a judgment in its favor on the post-PSP Fourth Amendment claim, the government claims that the issue it obtained judgment on, and all other post-PSP issues, are actually not in the case. But the government cannot accept the benefit of the Court's judgment in its favor on plaintiffs' constitutional challenge to its post-PSP conduct, yet simultaneously refuse to provide discovery on that very same post-PSP conduct so that plaintiffs may pursue their statutory claims. The Court's conclusion that post-PSP conduct is within the scope of the complaint was correct and remains the law of the case.

Plaintiffs request that the Court overrule the government's objections based on its attempt to limit the temporal scope of the complaint to pre-2007 PSP conduct.

**4. There Has Been No Discovery Abuse.** Plaintiffs have relied on RFAs and interrogatories to minimize the intrusiveness of their discovery requests and to avoid to the extent possible the necessity of depositions. Plaintiffs' RFAs are proper. They all address matters that are true and which should be beyond dispute. Indeed, the government has not denied a single RFA, even in part. Nor are the RFAs objectionable in form. Some are broad, some are highly specific. That an RFA is narrow, detailed, and specific does not make it compound, conjunctive, or disjunctive. Plaintiffs' interrogatories are also proper inquiries into the facts put in issue by their complaint.

The section 2712(b)(4) procedure ordered by the Court will protect national security. The government, in its classified submissions in the Fourth Amendment summary judgment briefing and its other classified submissions, has already provided the Court with extensive classified information regarding the same surveillance activities that are at issue in plaintiffs' discovery requests. The section 2712(b)(4) procedure, to which plaintiffs will have no access absent further order by the Court, will be equally protective of that information.

## The Government's Statement

Plaintiffs' discovery not only commits multiple abuses of the discovery process, it also seeks classified operational details about NSA intelligence activities that are absolutely protected from disclosure by statute; calls for enormous volumes of classified documents and information that are irrelevant to their statutory claims; and disregards the Court's prior decision upholding the Government's assertion of the state secrets privilege over the same information to which they now demand access. As an alternative to production, Plaintiffs propose that the Government—after preparing written responses to hundreds of discovery requests, and gathering all documents supporting each of their responses—should be required, under 50 U.S.C. § 1806(f), to deposit the entire mass of sensitive national security information on the Court's doorstep, for the Court to conduct its own *ex parte* review and determine whether Plaintiffs' statutory claims have merit. That “solution” addresses none of the intractable problems posed by their discovery requests.

Plaintiffs' request for an order compelling discovery should therefore be denied, and the Court instead should enter a protective order relieving the Government of any obligation to respond to their highly intrusive and burdensome requests.

**Abuse of Discovery Processes:** Any pretense that Plaintiffs attempted “to minimize the intrusiveness” of their discovery requests, *supra* at 5, is immediately shattered by their sheer number, exceeding 300, and the target at which the vast majority of Plaintiffs' requests take direct aim—the same operational details of classified NSA intelligence activities whose disclosure this Court has already ruled would place national security at risk. *See* Order Denying Pls.' Mot. for Partial Summ. Judg. [etc.] (Dkt. No. 321) (“Upstream Order”) at 8-9.

The main engine of Plaintiffs' discovery effort is a set of 190 requests for admissions (“RFAs”), the bulk of which seek information about alleged NSA copying and scanning (for targeted selectors) of electronic communications transiting the Internet. They are calculated to elicit information that Plaintiffs hope will confirm their theories regarding the sources and methods employed by the NSA, under the President's Surveillance Program (“PSP”), and FISC-authorized programs conducted under FISA, to obtain the contents of online communications.

Plaintiffs, however, do not limit their RFAs to simple inquiries about alleged copying and searching of their communications. The Government is also asked to admit or deny that it copies and searches (or copied and searched in the past) communications of AT&T customers generally, communications transiting AT&T's Internet facilities, and communications transiting facilities of other service providers. In addition, and of no discernible bearing on Plaintiffs' claims, the Government is asked to specify whether it copied and searched various types of communications, such as domestic communications, international communications, those sent or received in the United States, those sent or received by U.S. persons located in the United States, and those sent to or from specified foreign countries. Plaintiffs' RFAs also attempt to discover various operational details, such as whether or not particular categories of communications are (or were) copied and searched “at [AT&T's] Folsom Street Facility,” and “using fiber-optic splitters.”

Elements of each of thread of inquiry—whose communications were copied and searched, what kind, where, by what means, and on which providers' networks, all matters classified to protect national security—are interchanged from one RFA to the next, resulting in an endless series of tortuous inquiries that defy the sort of straightforward “admi[ssion] or den[ial] without explanation” that RFAs should be framed to allow. *Safeco of Am. v. Rawstron*,

181 F.R.D. 441, 447 (C.D. Cal. 1998). RFAs “should not contain compound, conjunctive, or disjunctive ... statements,” *James v. Maguire Corr. Facility*, 2012 WL 3939343, at \*4 (N.D. Cal. Sept. 10, 2012), yet, as illustrated below, Plaintiffs’ RFAs do not ask the Government to admit single statements of fact, but propound amalgamated inquiries having as many as 15 parts:

**REQUEST FOR ADMISSION NO. 134:** Admit that [1] during the PSP Period [2] You caused [3] the contents [4] of one or more [5] of the domestic communications [6] sent [7] or received [8] by Gregory Hicks and [9] copied [10] while in transmission [11] within the United States [12] to be searched [13] without any probable cause to believe or [14] individualized suspicion [15] that the communications searched contained the searched-for information.

Thus so, for nearly 190 RFAs, *see* Gov’t App. B, *infra* (select examples of Plaintiffs’ discovery requests), which in truth are not properly labeled as RFAs, but are used here as interrogatories, propounded to discover evidence supporting Plaintiffs’ theories regarding NSA intelligence-gathering operations. Contrary to Plaintiffs’ purpose, however, RFAs “are not a discovery device[.]” *K.C.R. v. Cty. of Los Angeles*, 2014 WL 3433925, at \*3 (C.D. Cal. July 14, 2014). “The purpose of Rule 36(a) is to expedite trial by establishing certain material facts as true and narrowing the range of issues for trial,” and therefore the rule “presupposes that the party propounding the requests [already] knows the facts set forth ....” *Suever v. Connell*, 2008 WL 906423, at \*13 (N.D. Cal. Apr. 1, 2008). Accordingly, “requests for admissions should not be used to establish facts which are obviously in dispute,” *James*, 2012 WL 3939343, at \*4, nor “as substitutes for discovery processes to uncover evidence.” *K.C.R.*, 2014 WL 3433925, at \*3.

Yet that is what Plaintiffs admit they have done, stating unabashedly that RFAs are the “form of discovery” [sic] on which they have “relied [most] heavily” to uncover evidence about alleged NSA copying and searching of online communications. Pls.’ App. A, *infra* at 11. The Court should not countenance this effort to pass off as RFAs what are in fact interrogatories, especially where the result, by design or otherwise, would be to exceed the numeric limit on interrogatories by a factor of nearly ten. *See* Fed. R. Civ. P. 33(a)(1); *Safeco*, 181 F.R.D. at 447.

Plaintiffs compound these abuses with their unduly burdensome and intrusive (Rule 33) interrogatories and requests for production of documents. While nominally within the limits of Rule 33(a)(1), in fact many of Plaintiffs’ 70 interrogatories contain multiple subparts each, thus swelling their true volume far in excess of the number permitted (not even accounting for the nearly 190 interrogatories they have attempted to disguise as RFAs). *See AngioScore, Inc. v. TriReme Med., Inc.*, 2014 WL 71887799, at \*6 (N.D. Cal. Dec. 16, 2014). They also focus directly on the details of NSA intelligence-gathering operations that the Court has already held cannot be disclosed without placing national security at risk. Nearly a dozen of them demand narrative responses “describ[ing] the process[es]” by which the NSA allegedly has “copied,” “filtered,” “searched,” and “acquired” “the contents of communications sent or received within the United States by AT&T customers while in transmission on the Internet.” Paired with these intrusive inquiries are a like number of requests for production of documents “sufficient to evidence” each of these highly sensitive and classified intelligence-gathering processes.

Adding further, and immensely, to these difficulties, Plaintiffs’ interrogatories demand written descriptions of all facts *and* documents supporting the Government’s responses to more than 40 of their compound and convoluted RFAs, and still more, that the Government produce all documents supporting its responses to all 190 of their RFAs and all 70 of their interrogatories.

No such attempt to rummage through documents and information so critical to the Nation's security has ever been condoned by the courts, and it should not be permitted here.

**Statutory Privilege Under 50 U.S.C. § 3605:** Even if it were possible to overlook Plaintiffs' abuses of the discovery process, their request to compel discovery should be denied for the fundamental reason that the information they seek is absolutely protected from disclosure by section 6 of the National Security Agency Act, 50 U.S.C. § 3605. Section 6 provides, with a narrow exception not pertinent here, that "nothing in this chapter [Title 50, U.S.C., ch. 47] or any other law ... shall be construed to require the disclosure of ... any function of the [NSA], or any information with respect to the activities thereof ..." Thus, Congress itself enacted a *statutory* privilege (not addressed by the Court's preemption ruling in *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1103-05 (N.D. Cal. 2013)) that affords "absolute" protection to information concerning NSA intelligence-gathering activities. *Linden v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996). Plaintiffs' requests for access to such information are unconditionally barred by Section 6, which was not implicitly repealed by 18 U.S.C. § 2712(b)(4), as Plaintiffs suggest, nor waived by the Government in prior proceedings that had nothing to do with discovery. *See supra* at 2 n.1.

**Lack of Relevance:** Plaintiffs' effort to probe into privileged and classified NSA intelligence programs, without regard for national security, is all the more dismaying because the information they insist on exposing is irrelevant to their claims. They contend that alleged in-transit copying of online communications (prior to scanning them for targeted selectors) itself violates the Wiretap Act, which prohibits unauthorized "intercept[ion]" of electronic communications, 18 U.S.C. § 2511(1)(a), defined as the "aural or other acquisition" of their contents, *id.*, § 2510(4). *Supra* at 3-4. That is so, Plaintiffs maintain, regardless of whether a copied communication is ingested into NSA databases. But cases actually considering the question hold that "acquisition" under the Wiretap Act requires actual human inspection of a communication's contents, or preservation of its contents making such review possible. *See, e.g., Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 742 (4<sup>th</sup> Cir. 1994). Hence, if a communication is electronically copied in transit but not found to contain targeted selectors, and so is instantaneously discarded, not ingested, then no acquisition under the Wiretap Act occurs. If on the other hand the copied communication contains one or more targeted selectors and is preserved in the NSA's databases for later analyst review, an acquisition has taken place. But the pivotal event in both cases is the retention of the copied communication (or not) for scrutiny of its contents by agency personnel, and whether the communication was copied beforehand is irrelevant to whether a Wiretap Act "acquisition" has occurred. *Noel v. Hall*, 568 F.3d 743 (9<sup>th</sup> Cir. 2009), on which Plaintiffs rely, does not address the circumstances alleged here.

Likewise, Plaintiffs' position that evidence of electronic scanning is relevant to claims for unauthorized "use" of their communications, *see* 18 U.S.C. § 2511(1)(d); *supra* at 4, ignores the fact that review of a communication, without more, does not constitute a "use" under the Wiretap Act. *E.g., Dorris v. Absher*, 179 F.3d 420, 426 (6<sup>th</sup> Cir. 1999) ("[L]istening alone is insufficient to impose [use] liability" under the Wiretap Act.).

Also misguided is the contention that discovery about bulk collection of communications records under the PSP is relevant to their claim under the Stored Communications Act. *Supra* at 4. Under the PSP the Government did not serve process "requir[ing]" companies to produce records within the meaning of 18 U.S.C. § 2703(c). *See U.S. v. Beckett*, 369 F. App'x 52, 55 (11<sup>th</sup> Cir. 2010) (distinguishing compelled from non-compelled disclosure under the SCA).



Plaintiffs' conjecture that information about alleged copying and searching of other persons' communications may provide circumstantial evidence to support their claims (where no acquisition of their communications is shown), *supra* at 4, rests on speculation about the scope of the NSA's programs; ignores the irrelevance of copying and scanning; and lays bare the essence of their discovery strategy—to expose NSA sources and methods, regardless of the risk to national security, in the distant hope of collecting damages for the imperceptible electronic copying and scanning of communications never disclosed to the Government.

To call it “improper” of the Government to contest the relevance of Plaintiffs' discovery to their statutory claims, *supra* at 3, ignores first principles. Rule 26(b)(1) defines the scope of discovery as “non-privileged matter that is relevant to any party's claim or defense . . .,” not information that propounding parties unilaterally regard as relevant. Where, as here, “there is an objection that discovery goes beyond material relevant to the parties' claims or defenses,” Rule 26 contemplates that “the court w[ill] become involved to determine whether [or not] the discovery is relevant to the claims or defenses.” Fed. R. Civ. P. 26(b)(1) (adv. cmte. note 2000); *see Thornton v. Crazy Horse, Inc.*, 2010 WL 3718945, at \*1 n.4 (D. Alaska Sept. 14, 2010). The Government's relevance objections ask nothing more.<sup>3</sup>

**State Secrets Privilege:** Finally, even if the information Plaintiffs seek were otherwise discoverable, it falls squarely within the scope of the assertion of the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1), already made in this case by the Director of National Intelligence. Plaintiffs are mistaken when they assert that the Court's interlocutory ruling in *Jewel*, 965 F. Supp. 2d at 1103-05, now compels the Government to waive its privilege. *Supra* at 2-3. The Court *upheld* the Government's assertion of privilege in its Upstream Order, at 8-9. It is not the Government but Plaintiffs, by endeavoring to compel disclosure of the very information addressed in that ruling, who seek to re-litigate an issue they have already lost.

To that end they now propose, in effect, that under 50 U.S.C. § 1806(f) the Government should prepare detailed written answers and assemble masses of documents (all classified at the highest levels) in response to hundreds of discovery requests; that the Attorney General should certify under oath, as to each response and document, that disclosure would harm national security; and that the Court should then be responsible for reviewing the entire resulting aggregation of classified documents and information, *ex parte*, to determine the merit of Plaintiffs' statutory claims, all without prior consideration of whether any of it is relevant to those claims in the first place. *Supra* at 3, 5. That is not what occurred when the Court upheld the Government's claim of privilege and refused to consider the merits of Plaintiffs' Fourth Amendment Upstream claim. And Plaintiffs' reliance now on § 2712(b)(4) does not alter the fact that regardless of the statutory or constitutional basis of their claims, attempting to address their claims would reveal information that the Court has already held is protected. Whatever the import of § 1806(f) and § 2712(b)(4) in cases to which they pertain, they were not meant to displace the Government's privileges, and cannot practicably be applied, in cases such as this.

The Court should deny Plaintiffs' request for an order compelling discovery, and enter a protective order relieving the Government of any further obligation to respond to their requests.

---

<sup>3</sup> Plaintiffs are correct that the Government also objects to requests for information about FISC-authorized programs conducted after conclusion of the PSP as beyond the scope of the activities alleged in the Complaint. *See supra* at 5. Contrary to Plaintiffs' argument, the Court has not resolved this “scope of Complaint” issue.

**COUNSEL FOR PLAINTIFFS:**

s/ Richard R. Wiebe

Cindy Cohn (SBN 145997)  
cindy@eff.org  
David Greene (SBN 160107)  
Lee Tien (SBN 148216)  
Kurt Opsahl (SBN 191303)  
Mark Rumold (SBN 279060)  
Andrew Crocker (SBN 291596)  
Jamie L. Williams (SBN 279046)  
James S. Tyre (SBN 083117)  
ELECTRONIC FRONTIER  
FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
Telephone: (415) 436-9333  
Fax: (415) 436-9993

Richard R. Wiebe (SBN 121156)  
wiebe@pacbell.net  
LAW OFFICE OF RICHARD R. WIEBE  
One California Street, Suite 900  
San Francisco, CA 94111  
Telephone: (415) 433-3200  
Fax: (415) 433-6382

Rachael E. Meny (SBN 178514)  
rmeny@kvn.com  
Michael S. Kwun (SBN 198945)  
Benjamin W. Berkowitz (SBN 244441)  
Audrey Walton-Hadlock (SBN 250574)  
Justina K. Sessions (SBN 270914)  
Philip J. Tassin (SBN 287787)  
KEKER & VAN NEST, LLP  
633 Battery Street  
San Francisco, CA 94111  
Telephone: (415) 391-5400  
Fax: (415) 397-7188

Thomas E. Moore III (SBN 115107)  
tmoore@rroyselaw.com  
ROYSE LAW FIRM, PC  
1717 Embarcadero Road  
Palo Alto, CA 94303  
Telephone: (650) 813-9700  
Fax: (650) 813-9777

Aram Antaramian (SBN 239070)  
aram@eff.org  
LAW OFFICE OF ARAM ANTARAMIAN  
1714 Blake Street  
Berkeley, CA 94703  
Telephone: (510) 289-1626

**COUNSEL FOR THE  
GOVERNMENT DEFENDANTS:**

s/ James J. Gilligan

Benjamin C. Mizer  
Principal Deputy 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](mailto:james.gilligan@usdoj.gov)

Rodney Patton  
Senior Counsel

Julia A. Berman  
Timothy A. Johnson  
Trial Attorneys

U.S. DEPARTMENT OF JUSTICE,  
CIVIL DIVISION  
20 Massachusetts Avenue, NW, Rm. 6102  
Washington, D.C. 20001  
Telephone: (202) 514-3358  
Fax: (202) 616-8470

## **Plaintiffs' Appendix A**

In serving their discovery requests on the government defendants, plaintiffs' goal was to minimize the intrusiveness of their requests and to avoid if possible the necessity of depositions of government witnesses. In particular, plaintiffs relied heavily on requests for admission ("RFA"). RFAs are the least intrusive form of discovery. An RFA focuses on a single matter, which may be admitted, partially admitted, or denied without revealing any collateral information. Most of plaintiffs' RFAs were directed at the government's copying and searching of communications and its collection and searching of communications records, both during the pre-2007 "President's Surveillance Program" ("PSP") and during post-PSP surveillance activities such as the government's "Upstream" Internet surveillance and its bulk collection of telephone records under section 215 of FISA.

Plaintiffs also served interrogatories. Some interrogatories addressed the copying, filtering, and searching of communications and the collection of communication records. Other interrogatories were tied to selected RFAs and conditional on the government's denial of the particular RFA: if the government denied the RFA, the corresponding interrogatory asked the government to explain the basis for its denial. Some interrogatories inquired into the basis for the government defendants' denial of allegations of the Complaint or the basis for any defense or justification.

Plaintiffs served document requests as well. Some document requests addressed the copying, filtering, and searching of communications and the collection of communication records. Others addressed the allegations of the Complaint or the basis for any defense or justification. Some addressed the government defendants' RFA and interrogatory responses, and some requested specific documents.

### **I. General Structure of Plaintiffs' Discovery Requests**

#### **A. Requests For Admission**

Plaintiffs served 190 RFAs, organized into the following topics and subtopics.

1. The copying of communications during the PSP period.

a. Plaintiffs' communications:

RFAs 1, 2, 33 to 37, 51 to 58, 64 to 71, 79 to 86, 92 to 99, 107 to 114, 122 to 129.

b. Communications transiting Folsom Street and other AT&T facilities, and communications of AT&T customers:

RFAs 5, 6, 9, 10 to 13, 16, 17, 22, 23, 27, 28, 32.

c. Communications transiting facilities of electronic communications service providers generally:

RFAs 26, 28, 29, 30, 31.

2. The searching of communications during the PSP period.

a. Plaintiffs' communications:

RFAs 3, 4, 42 to 46, 59, 60 to 63, 72 to 78, 87 to 91, 100 to 106, 115 to 121, 130 to 134.

b. Communications transiting Folsom Street and other AT&T facilities, and communications of AT&T customers:

RFAs 7, 8, 14, 15, 18 to 21, 24, 25, 41, 47.

c. Communications transiting facilities of electronic communications service providers generally:

RFAs 38, 39, 40, 41, 48, 49, 50.

3. The copying of communications during the post-PSP, "Upstream" period.

a. Plaintiffs' communications:

RFAs 152, 155.

b. Communications transiting Folsom Street and other AT&T facilities, and communications of AT&T customers:

RFAs 137, 138.

c. Communications transiting facilities of electronic communications service providers generally:

RFAs 135, 136, 139, 140, 142 to 144.

4. The filtering of communications during the post-PSP, "Upstream" period.

RFAs 145 to 148, 153, 156.

5. The searching of communications during the post-PSP, “Upstream” period.
  - a. Plaintiffs’ communications:

RFAs 154, 157.
  - b. Communications transiting facilities of electronic communications service providers generally:

RFAs 141, 149 to 151, 154, 158 to 160.
6. Collection of communications records.
  - a. Collection of communications records during the PSP period:

RFAs 162 to 168.
  - a. Post-PSP collection of communications records:

RFAs 169 to 175.
7. Document-based RFAs.
  - a. Draft NSA Inspector General Report on the PSP (ECF No. 147, Ex. A):

RFAs 176 to 178.
  - b. Exhibits to the Mark Klein Declaration (ECF No. 84):

RFAs 179 to 187.
8. Miscellaneous:

RFAs 161, 188 to 190.

**B. Interrogatories**

Plaintiff Knutzen served 24 interrogatories, Plaintiff Jewel served 23 interrogatories, and Plaintiff Walton served 23 interrogatories on the following topics.

1. The copying of communications during the PSP period:

Knutzen interrogatories 1, 2, 6.
2. The filtering of communications during the PSP period:

Knutzen interrogatory 3.
3. The searching of communications during the PSP period:

Knutzen interrogatory 4.

4. The searching of plaintiffs' communications at any time:

Knutzen interrogatories 7, 8, 17.

5. AT&T's Folsom Street Facility:

Knutzen interrogatories 5, 13.

6. The copying of communications during the post-PSP, "Upstream" period:

Knutzen interrogatories 9, 10, 14.

7. The filtering of communications during the post-PSP, "Upstream" period:

Knutzen interrogatory 11.

8. The searching of communications during the post-PSP, "Upstream" period:

Knutzen interrogatories 12, 15.

9. The copying of communications at any time:

Knutzen interrogatory 16.

10. Legal justifications for copying and searching communications:

Knutzen interrogatories 18 to 21.

11. Collection of communications records.

a. Collection of communications records during the PSP period:

Knutzen interrogatories 22, 23.

a. Collection of communications records at any time:

Knutzen interrogatory 24.

Jewel interrogatories 1, 2.

12. Interrogatories asking for the basis on which the government defendants have denied a particular RFA:

Jewel interrogatories 3 to 23.

Walton interrogatories 1 to 19.

13. Interrogatories inquiring into the basis for the government defendants' denial of any allegations of Counts 9, 12, and 15 of the Complaint and the basis for any affirmative defense:

Walton interrogatories 20 to 23.

### C. Document Requests

Plaintiffs served 42 document requests on the following topics.

1. Documents sufficient to evidence the copying, filtering, and searching of communications during the PSP period:

Document requests 1 to 7.

2. Documents sufficient to evidence the copying, filtering, and searching of communications during the post-PSP “Upstream” period:

Document requests 8 to 14.

3. Documents sufficient to evidence the collection of communications records during the PSP period:

Document requests 15, 16.

4. Documents sufficient to evidence the collection of communications records at any time:

Document requests 17 to 19.

5. Documents on which the government defendants may rely to deny any allegation of Counts 9, 12, 15 of the Complaint or to support any defense, privilege, or immunity:

Document requests 20 to 23.

6. Documents relating to the presence or absence of warrants, court orders, probable cause, individualized suspicion, or other justification:

Document requests 24 to 33.

7. Documents supporting the government defendants’ denial of any RFA and their interrogatory responses:

Document requests 34 to 37.

8. Requests for specific FISC orders, memoranda by DOJ Office of Legal Counsel attorneys John Yoo and Jack Goldsmith, and draft NSA Inspector General Report on the PSP:

Document requests 38 to 42.

## II. Defendants' Objections

### A. Plaintiffs' discovery requests to which the government has made state secrets objections:

1. RFA General Objections 3, 10; RFAs 1 to 188.
2. Interrogatories.
  - a. Knutzen interrogatories: General objections 4, 10; interrogatories 1 to 24.
  - b. Jewel interrogatories: General objections 4, 10; interrogatories 1 to 23.
  - c. Walton interrogatories: General objections 4, 10; interrogatories 1 to 23.
3. Document requests: General objections 4, 10; requests 1 to 42.

### B. Plaintiffs' discovery requests to which the government has made relevance objections based on the government's statutory interpretations:

1. RFA General Objections 4, 7, 8; RFAs 1 to 157, 162 to 169.
2. Interrogatories.
  - a. Knutzen interrogatories: General objections 3, 7, 8; interrogatories 1 to 24.
  - b. Jewel interrogatories: General objections 3, 7, 8; interrogatories 1 to 23.
  - c. Walton interrogatories: General objections 3, 7, 8; interrogatories 1 to 14.
3. Document requests: General objections 3, 7, 8; requests 1 to 19, 24 to 26, 28 to 37.

### C. Plaintiffs' discovery requests to which the government has made temporal scope-of-the-complaint objections:

1. RFAs 135 to 157, 169 to 175.
2. Interrogatories.
  - a. Knutzen interrogatories 9 to 23.
  - b. Jewel interrogatories 1, 2.
  - c. Walton interrogatories 7 to 9, 15 to 19.
3. Document requests 8 to 19, 23 to 37.



## Government's Appendix B

The following are examples of Plaintiffs' more than 300 discovery requests illustrating points made in the Government's Statement, above.

### **Plaintiffs' First Set of Requests for Admission**

**REQUEST FOR ADMISSION NO. 5:** Admit that during the PSP Period You procured AT&T to copy all electronic communications at the Folsom Street Facility transiting between AT&T's Internet facilities and the Internet facilities of non-AT&T electronic communications service providers.

**REQUEST FOR ADMISSION NO. 6:** Admit that the PSP Copied Communications made at the Folsom Street Facility included electronic communications sent or received within the United States by AT&T customers.

**REQUEST FOR ADMISSION NO. 8:** Admit that the PSP Copied Communications made at the Folsom Street Facility whose contents You searched or caused to be searched included electronic communications sent or received within the United States by AT&T customers.

**REQUEST FOR ADMISSION NO. 10:** Admit that fiber-optic splitters installed at the Folsom Street Facility were used during the PSP Period to copy the contents of all the electronic communications transiting between AT&T's Internet facilities and the Internet facilities of other electronic communications service providers.

**REQUEST FOR ADMISSION NO. 11:** Admit that fiber-optic splitters installed at the Folsom Street Facility were used during the PSP Period to copy the contents of electronic communications of AT&T domestic customers while in transmission over the Internet.

**REQUEST FOR ADMISSION NO. 12:** Admit that during the PSP Period You caused AT&T to copy by the use of a device at the Folsom Street Facility domestic and international electronic communications sent or received in the United States by AT&T customers while in transmission over the Internet without any warrant or court order authorizing You to do so.

**REQUEST FOR ADMISSION NO. 13:** Admit that during the PSP Period You caused AT&T to copy by the use of a device at the Folsom Street Facility domestic and international electronic communications sent or received in the United States by AT&T customers while in transmission over the Internet without any probable cause to believe or individualized suspicion that the communication copied contained a tasked selector.

**REQUEST FOR ADMISSION NO. 18:** Admit that during the PSP Period You caused the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States by use of a device while in transmission over AT&T's Internet facilities to be searched without any warrant or court order authorizing You to do so.

**REQUEST FOR ADMISSION NO. 19:** Admit that during the PSP Period You caused the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States by use of a device while in transmission over AT&T's Internet facilities to be searched without any probable cause to believe or individualized suspicion that the searched communication contained the searched-for information.

**REQUEST FOR ADMISSION NO. 20:** Admit that during the PSP Period You caused the contents of all electronic communications that were sent or received within the United States by AT&T customers and copied within the United States by use of a device while in transmission over AT&T's Internet facilities, and that You or AT&T determined were likely to be international communications, to be searched without any warrant or court order authorizing You to do so.

**REQUEST FOR ADMISSION NO. 25:** Admit that during the PSP Period in response to Your request for assistance AT&T searched the contents of electronic communications sent or received within the United States by AT&T domestic customers and copied within the United States by use of a device while in transmission, with no probable cause to believe or individualized suspicion that each communication searched contained the searched-for information.

**REQUEST FOR ADMISSION NO. 49:** Admit that during the PSP Period You caused the contents of all electronic communications copied at the United States facilities of electronic communications service providers and sent to or received by United States persons within the United States, and that You or the electronic communications service provider determined were likely to be international communications, to be searched without any warrant or court order authorizing You to do so.

**REQUEST FOR ADMISSION NO. 62:** Admit that during the PSP Period You caused the contents of one or more of the international electronic communications sent or received by each plaintiff in the United States and copied while in transmission within the United States to be searched without any probable cause to believe or individualized suspicion that each communication searched contained the searched-for information.

**REQUEST FOR ADMISSION NO. 103:** Admit that the contents of international electronic communications sent or received by plaintiff Knutzen between the United States and New Zealand, the Netherlands, Denmark, and South Africa and copied while in transmission within the United States were among the communications You caused to be searched during the PSP Period without any warrant or court order authorizing You to do so.

**REQUEST FOR ADMISSION NO. 121:** Admit that the contents of international electronic communications sent or received by plaintiff Walton between the United States and Taiwan, Canada, France, Germany, the United Kingdom, Spain, and Saudi Arabia and copied while in transmission within the United States were among the communications You caused to be searched during the PSP Period without any probable cause to believe or individualized suspicion that each communication searched contained the searched-for information.

**REQUEST FOR ADMISSION NO. 152:** Admit that international electronic communications sent or received within the United States by plaintiffs are copied in Your upstream collection process.

**REQUEST FOR ADMISSION NO. 154:** Admit that the contents of international electronic communications sent or received within the United States by plaintiffs are searched for selectors in Your upstream collection process.

**REQUEST FOR ADMISSION NO. 155:** Admit that international electronic communications between the United States and the countries of the United Kingdom, Germany, Indonesia, New Zealand, Australia, the Netherlands, Denmark, South Africa, Taiwan, Canada, France, Spain, and Saudi Arabia that are sent or received within the United States by plaintiffs are copied in Your upstream collection process.

**REQUEST FOR ADMISSION NO. 157:** Admit that the contents of international electronic communications between the United States and the countries of the United Kingdom, Germany, Indonesia, New Zealand, Australia, the Netherlands, Denmark, South Africa, Taiwan, Canada, France, Spain, and Saudi Arabia that are sent or received within the United States by plaintiffs are searched for selectors in Your upstream collection process.

**REQUEST FOR ADMISSION NO. 162:** Admit that during the PSP Period You caused AT&T to disclose to You, in bulk, records and other information pertaining to subscribers or customers of its electronic communications services or remote computing services facilities without any warrant or court order or subpoena authorizing the disclosure.

**REQUEST FOR ADMISSION NO. 169:** Admit that from July 2004 to June 2015 You caused AT&T to disclose to You, in bulk, records and other information pertaining to subscribers or customers of its electronic communications services or remote computing services facilities on authority of orders issued by the Foreign Intelligence Surveillance Court.

### **Plaintiffs' Interrogatories**

**(three sets served in the names of plaintiffs Knutzen, Jewel, and Walton)**

**[KNUTZEN] INTERROGATORY NO. 2:** Describe the process by which during the PSP Period You or any other person or entity procured by You copied within the United States the contents of electronic communications sent or received within the United States by AT&T customers while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Document Request No. 2, below.*]

**[KNUTZEN] INTERROGATORY NO. 4:** Describe the process by which during the PSP Period You or any other person or entity procured by You searched the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Document Request No. 4, below.*]

**[KNUTZEN] INTERROGATORY NO. 6:** Identify the number of each plaintiff's electronic communications You copied or procured to be copied or caused to be copied within the United States by the use of a device during the PSP Period while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Document Request No. 6, below.*]

**[KNUTZEN] INTERROGATORY NO. 8:** Identify the number of each plaintiff's electronic communications You caused to be searched without any probable cause to believe or individualized suspicion that the searched communication contained the searched-for information. [*See also Document Request No. 7, below.*]

**[KNUTZEN] INTERROGATORY NO. 10:** Describe the process by which in Your upstream collection You or any other person or entity copy within the United States the contents of electronic communications sent or received within the United States by AT&T customers while in transmission over the Internet. [*See also Document Request No. 9, below.*]

**[KNUTZEN] INTERROGATORY NO. 12:** Describe the process by which in Your upstream collection You or any other person or entity search the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States while in transmission over the Internet. [*See also Document Request No. 11, below.*]

**[KNUTZEN] INTERROGATORY NO. 14:** Identify the number of each plaintiff's electronic communications You copied or procured to be copied or caused to be copied within the United States by the use of a device while in transmission over the Internet as part of Your upstream collection. [*See also Document Request No. 13, below.*]

**[KNUTZEN] INTERROGATORY NO. 15:** Identify the number of each plaintiff's electronic communications You searched or procured to be searched or caused to be searched as part of Your upstream collection. [*See also Document Request No. 14, below.*]

**[KNUTZEN] INTERROGATORY NO. 22:** Describe the process by which during the PSP Period You obtained any records or other information pertaining to subscribers or customers of AT&T's electronic communications services or remote computing services without any warrant or court order or subpoena authorizing the disclosure. [*See also Document Request No. 15, below.*]

**[KNUTZEN] INTERROGATORY NO. 24:** Describe each disclosure to You, pursuant to a process of bulk collection, of any records or other information pertaining to subscribers or customers of AT&T's electronic communications services or remote computing services. [*See also Document Request No. 17, below.*]

**[JEWEL] INTERROGATORY NO. 1:** Describe each disclosure to You, pursuant to a process of bulk collection, of any records or other information pertaining to plaintiffs' use of AT&T's electronic communications services or remote computing services, including telephone call records, other telephone call information, Internet records, Internet metadata, or other Internet information pertaining to each plaintiff. [*See also Document Request No. 18, below.*]

**[JEWEL] INTERROGATORY NO. 9:** If Your response to Request for Admission No. 18 of Plaintiffs' First Set of Requests for Admission is anything other than an unqualified admission, describe all facts and documents upon which You base Your response. If Your response instead is an unqualified admission, do not respond to this interrogatory.

**[JEWEL] INTERROGATORY NO. 10:** If Your response to Request for Admission No. 19 of Plaintiffs' First Set of Requests for Admission is anything other than an unqualified admission, describe all facts and documents upon which You base Your response. If Your response instead is an unqualified admission, do not respond to this interrogatory.

**[WALTON] INTERROGATORY NO. 6:** If Your response to Request for Admission No. 62 of Plaintiffs' First Set of Requests for Admission is anything other than an unqualified admission, describe all facts and documents upon which You base Your response. If Your response instead is an unqualified admission, do not respond to this interrogatory.

**[WALTON] INTERROGATORY NO. 7:** If Your response to Request for Admission No. 152 of Plaintiffs' First Set of Requests for Admission is anything other than an unqualified admission, describe all facts and documents upon which You base Your response. If Your response instead is an unqualified admission, do not respond to this interrogatory.

**[WALTON] INTERROGATORY NO. 9:** If Your response to Request for Admission No. 154 of Plaintiffs' First Set of Requests for Admission is anything other than an unqualified admission, describe all facts and documents upon which You base Your response. If Your response instead is an unqualified admission, do not respond to this interrogatory.

### **Plaintiffs' Requests for Production**

**DOCUMENT REQUEST NO. 2:** Documents sufficient to evidence the process by which at any time during the PSP Period You or any person or entity procured by You copied within the United States the contents of electronic communications sent or received within the United States by AT&T customers while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Knutzen Interrogatory No. 2, above.*]

**DOCUMENT REQUEST NO. 4:** Documents sufficient to evidence the process by which at any time during the PSP Period You or any person or entity procured by You searched the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Knutzen Interrogatory No. 4, above.*]

**DOCUMENT REQUEST NO. 6:** Documents sufficient to evidence for each plaintiff the number of that plaintiff's electronic communications You copied or procured to be copied or caused to be copied within the United States by the use of a device during the PSP Period while in transmission over the Internet without any warrant or court order authorizing You to do so. [*See also Knutzen Interrogatory No. 6, above.*]

**DOCUMENT REQUEST NO. 7:** Documents sufficient to evidence the number of each plaintiff's Copied Communications You caused to be searched. [*See also Knutzen Interrogatory No. 8, above.*]

**DOCUMENT REQUEST NO. 9:** Documents sufficient to evidence the process by which in Your upstream collection You or any person or entity copy within the United States the contents of electronic communications sent or received within the United States by AT&T customers while in transmission over the Internet. [*See also Knutzen Interrogatory No. 10, above.*]

**DOCUMENT REQUEST NO. 11:** Documents sufficient to evidence the process by which in Your upstream collection You or any person or entity search the contents of electronic communications sent or received within the United States by AT&T customers and copied within the United States while in transmission over the Internet. [*See also Knutzen Interrogatory No. 12, above.*]

**DOCUMENT REQUEST NO. 13:** Documents sufficient to evidence for each plaintiff the number of that plaintiff's electronic communications You copied or procured to be copied or caused to be copied within the United States by the use of a device while in transmission over the Internet as part of Your upstream collection. [*See also Knutzen Interrogatory No. 14, above.*]

**DOCUMENT REQUEST NO. 14:** Documents sufficient to evidence for each plaintiff the number of that plaintiff's electronic communications You searched or procured to be searched or caused to be searched as part of Your upstream collection. [*See also Knutzen Interrogatory No. 15, above.*]

**DOCUMENT REQUEST NO. 15:** Documents sufficient to evidence the process by which at any time during the PSP Period You obtained any records or other information pertaining to subscribers or customers of AT&T's electronic communications services or remote computing services without any warrant or court order or subpoena authorizing the disclosure. [*See also Knutzen Interrogatory No. 22, above.*]

**DOCUMENT REQUEST NO. 17:** Documents sufficient to evidence each disclosure to You, pursuant to a process of bulk collection, of any records or other information pertaining to subscribers of AT&T's electronic communications services or remote computing services. [*See also Knutzen Interrogatory No. 24, above.*]

**DOCUMENT REQUEST NO. 18:** Documents sufficient to evidence each disclosure to You, pursuant to a process of bulk collection, of any records or other information pertaining to plaintiffs' use of AT&T's electronic communications services or remote computing services, including telephone call records, other telephone call information, Internet records, Internet metadata, or other Internet information pertaining to each plaintiff. [*See also Jewel Interrogatory No. 1, above.*]

**DOCUMENT REQUEST NO. 34:** For each response by You to plaintiffs' First Set of Requests for Admission that is not an unqualified admission, any documents which support Your response.

**DOCUMENT REQUEST NO. 35:** For each response by You to plaintiff Erik Knutzen's First Set of Interrogatories, any documents which support Your response.

**DOCUMENT REQUEST NO. 36:** For each response by You to plaintiff Carolyn Jewel's First Set of Interrogatories, any documents which support Your response.

**DOCUMENT REQUEST NO. 37:** For each response by You to plaintiff Joice Walton's First Set of Interrogatories, any documents which support Your response.

**CIVIL L.R. 5-1 CERTIFICATION**

I attest that I have obtained the concurrence of James Gilligan (counsel for the Government Defendants) in the filing of this document.

/s/ Richard R. Wiebe

RICHARD R. WIEBE