CINDY COHN (SBN 145997)
cindy@eff.org
DAVID GREENE (SBN 160107)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
ANDREW CROCKER (SBN 291596)
JAMIE L. WILLIAMS (SBN 279046)
AARON MACKEY (SBN 286647)
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
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@keker.com
BENJAMIN W. BERKOWITZ (SBN 244441)
PHILIP J. TASSIN (SBN 287787)
KEKER, VAN NEST & PETERS, 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
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700
Fax: (650) 813-9777

ARAM ANTARAMIAN (SBN 239070)
antaramian@sonic.net
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

| | |
|---|---|
| CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | CASE NO. 08-CV-4373-JSW<br><br>**PLAINTIFFS' REPLY RE: THE GOVERNMENT'S SUMMARY JUDGMENT MOTION AND PLAINTIFFS' MOTION TO PROCEED TO RESOLUTION ON THE MERITS USING THE PROCEDURES OF SECTION 1806(f)**<br><br>Courtroom 5, Second Floor<br>The Honorable Jeffrey S. White |

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Rules**



**Other Authorities**

## INTRODUCTION

The parties' currently pending motions present two sides of the same coin: Does the body of evidence put forward by plaintiffs sufficiently establish their standing to defeat summary judgment and entitle them to move forward on the merits using classified evidence reviewed by the Court *ex parte* and *in camera*?

The government admits, and it is common knowledge, that it has tapped into the Internet backbone and has engaged in bulk collection of telephone records and Internet metadata over many years, surveilling billions of Internet and telephone communications. But the government claims that no one has standing to challenge the legality of that surveillance unless they can prove that a specific communication or record of theirs was among the billions of communications and records subjected to surveillance, and can also explain exactly how the surveillance was conducted. It claims that this standing requirement puts the surveillance beyond judicial review, even though this Court has ample information to adjudicate the issues and all the world knows the government engages in mass surveillance that has touched the communications of hundreds of millions of innocent people over the past 18 years.

The government's position, not surprisingly, is incorrect. Standing requires only an "identifiable trifle" of an injury-in-fact; a showing that it is more likely than not that the government interfered with at least one of each plaintiff's communications and records. A detailed explanation of the particular mechanism by which the government accomplished its surveillance is unnecessary.

As plaintiffs' opening brief demonstrates, the public evidence alone is more than sufficient to establish their standing. This standing entitles plaintiffs to move forward to a decision on merits in which the Court will use all of the evidence, both public and classified.

1. The public evidence amply demonstrates injury-in-fact:

   - Plaintiffs are telephone customers of AT&T and Verizon, and the evidence showing the government collected the phone records of all the customers of those companies conclusively establishes plaintiffs' standing for their phone records claims.
   - Plaintiffs' public evidence, including the testimony of four experts, also establishes

that at least one of their Internet communications more likely than not has been subjected to the admitted Internet backbone surveillance devices. This establishes their standing even if none of their communications were permanently retained.

- Plaintiffs' public evidence also establishes that at least one of their Internet metadata records was included in what the Foreign Intelligence Surveillance Court described as the "massive" and "wholly non-targeted bulk production" of Internet metadata.

2. Plaintiffs' public evidence is competent and admissible, and the government's objections lack merit for the reasons shown below.

3. The essence of the government's position is that in surveillance cases a plaintiff can establish standing only if there is a direct public admission by the government that the plaintiff has been surveilled. But that is not the law, either with respect to standing in general or plaintiffs' claims under in particular. Standing does not require a confession by the defendant, but may be proved by circumstantial evidence. And Congress did not make the government the gatekeeper of claims under 18 U.S.C. section 2712, permitting only claims that the government approves.

4. The classified evidence, construed in the light most favorable to plaintiffs and drawing all inferences in plaintiffs' favor, likely contains even more evidence supporting plaintiffs' standing. For example, it should show plaintiffs' individual phone records among the billions of phone records obtained by the government. And a full disclosure of the government's surveillance architecture for Internet communications would demonstrate that over the years at least one of each plaintiffs' communications was subjected to it.

5. Both for purposes of standing and for purposes of future proceedings on the merits, plaintiffs have demonstrated their entitlement to have the Court use the classified evidence *ex parte* and *in camera* to decide the issues before it. Section 2712(b)(4) requires the Court to use the classified evidence "[n]otwithstanding any other provision of law." 18 U.S.C. § 2712(b)(4). Plaintiffs satisfy any proposed standard for using classified evidence pursuant to section 2712 or 50 U.S.C. § 1806(f):

- Plaintiffs are aggrieved persons under the standard adopted by this Court in the related *In re NSA* multidistrict litigation because their "allegations 'are sufficiently

definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.'" *In re NSA Telecom. Records Litigation*, 595 F. Supp. 2d 1077, 1085 (N.D. Cal. 2009).

- Plaintiffs are aggrieved persons under the *Wikimedia* standard because they have "adduce[d] evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance." *Wikimedia Found. v. NSA/CSS*, 2018 WL 3973016, *8 (D. Md. Aug. 20, 2018).
- Plaintiffs are aggrieved persons under the government's standard because the evidence that shows their standing also shows that their Internet communications have been subjected to electronic surveillance and that their phone records and Internet metadata have been collected.
- Plaintiffs are aggrieved persons under the "zone of interests" test because they come within the zone of interests of the Wiretap Act, the Stored Communications Act ("SCA"), and section 2712.

Accordingly, the Court should deny the government's summary judgment motion and proceed to the merits, using the classified evidence as Congress has commanded.

## ARGUMENT

### I. Plaintiffs Have Proffered Sufficient Public Evidence Of Their Standing To Defeat Summary Judgment And To Proceed To The Merits Using Classified Evidence

The government's attack on the sufficiency of plaintiffs' evidence makes three critical errors.

First, the government contends that much of plaintiffs' evidence is inadmissible and should be disregarded. But plaintiffs' public evidence is admissible and sufficient to defeat summary judgment and to move forward on the merits, for the reasons explained in the sections that follow. The same evidence shows they are aggrieved for purposes of sections 2712(b)(4) and 1806(f).

Moreover, plaintiffs' evidence need not presently be in an admissible form to defeat summary judgment. Only if at trial the evidence "cannot be presented in a form that would be admissible in evidence" may it be disregarded at summary judgment. Fed. R. Civ. Pro. 56(c)(2).

"At the summary judgment stage, we do not focus on the admissibility of the evidence's form. We instead focus on the admissibility of its contents." *Fraser v. Goodale*, 342 F.3d 1032, 1036 (9th Cir. 2003). This is true for hearsay as well. "Even the declarations that do contain hearsay are admissible for summary judgment purposes because they 'could be presented in an admissible form at trial.'" *Fonseca v. Sysco Food Servs. of Arizona, Inc.*, 374 F.3d 840, 846 (9th Cir. 2004).

Second, despite the admonition that all reasonable inferences must be construed in favor of the non-moving party, the government mistakenly interprets the evidence in the manner most favorable to it, rather than to plaintiffs. *Pavoni v. Chrysler Group*, 789 F.3d 1095, 1098 (9th Cir. 2015) (on summary judgment, the court must "[v]iew[] the evidence . . . 'in the light most favorable to the party opposing the motion'").

Third, the government addresses each item of evidence in isolation, rather than weighing them together as they must be. The evidence must be considered as a whole; no single piece of evidence need carry the entire weight of showing plaintiffs' injuries. *Pavoni*, 789 F.3d at 1098 (on summary judgment, the court must "[v]iew[] the evidence 'as a whole'").

**A. Plaintiffs Have Standing To Challenge The Collection Of Their Phone Records**

Plaintiffs' evidence is sufficient to show that their phone records were collected as part of the government's bulk collection. The government does not dispute that if there is evidence that AT&T or Verizon participated in the phone records program, then plaintiffs have standing.

Plaintiffs have produced such evidence in the form of a letter (the "NSA Letter") from the NSA to the FISC that was included as Appendix C to the NSA Inspector General Report "Audit Report of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records—Control Weaknesses (ST-1.0-0004C)," dated September 29, 2010. ECF No. 417-4, Ex. B at p. 28. The NSA Letter, and the NSA Inspector General report to which it was attached, were produced by the Justice Department to the New York Times in FOIA litigation requesting only NSA Inspector General Reports. *Id.*, Ex. B at p. 1 (FOIA production cover letter from the U.S. Attorney's Office for the Southern District of New York); *New York Times v. NSA*, No. 15-cv-2383 (S.D.N.Y. Mar. 31, 2015), Complaint (ECF No. 1), ¶ 9; Scheduling Order (ECF No. 10); Declaration of David McCraw, ¶¶ 2-3, 5-6.

To its discredit, the government now questions the authenticity of the NSA Letter. It is truly disappointing, and deeply corrosive to the pursuit of justice, that the same Justice Department that in FOIA litigation in the Southern District of New York produced the NSA Letter on behalf of the NSA now stands before this Court and denies the authenticity of what it produced. This tactic is far beneath the standards of the Justice Department.

The government's authenticity challenge is meritless. Authentication "'does not erect a particularly high hurdle.'" *U.S. v. Dhinsa*, 243 F.3d 635, 658 (2d Cir. 2001). "The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances" can be "sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a), (b)(4). The appearance, contents, substance, internal patterns, and other distinctive characteristics of the NSA Letter and the NSA Inspector General's Report of which it is a part, taken together with the circumstances of its production by the government in FOIA litigation seeking only NSA Inspector General Reports, is sufficient to authenticate the NSA Letter. Indeed, the government's production of the NSA Letter is by itself a judicial admission of its authenticity. *Orr v. Bank of America*, 285 F.3d 764, 777 n.20 (9th Cir. 2002). And, if more is needed, counsel for the New York Times in its FOIA litigation against the NSA confirms that the NSA Letter was produced by the NSA. McCraw Decl. ¶¶ 5-6.

The NSA Letter is sufficient to show plaintiffs' standing. As the Court has held, when mass surveillance is aimed at all of a telecommunications provider's customers, all have standing to challenge it. *Jewel v. NSA*, 2015 WL 545925, *3-*4 (N.D. Cal. Feb. 10, 2015).

The NSA OIG Draft Report, authenticated by Edward Snowden, further confirms AT&T and Verizon's participation in the phone records program. ECF No. 147, Ex. A at 27-29, 33-34; ECF No. 417 at 9 n.6; Declaration of Edward Snowden, ¶¶ 2-5.

Plaintiffs' additional evidence also supports their standing. Plaintiffs were AT&T and Verizon customers. The government objects to the conclusion—a deduction based on evidence, not speculation—that a phone records program that excluded both AT&T (with 163 million

customer phone lines)[1] and Verizon (with 128 million customer phone lines)[2] could not perform three-hop contact chaining reliably, and certainly could not perform three-hop searches yielding the phone records of 120 million persons, as the PCLOB estimated occurred in 2012. ECF No. 417-2, Ex. A ("PCLOB 215 Report") at 30-31. But no other conclusion is mathematically possible, for there is no other phone company in America with anywhere near 120 million customers.[3] *See* ECF No. 417-3, Ex. A ("PR/TT Order") at 74 (phone records program involved "major telephone service providers").

On summary judgment, if an inference favors the non-moving party, it must be drawn unless it is unreasonable. The government acknowledges that the evidence in the preceding paragraph supports the inference that AT&T and Verizon participated in the phone records program and does not argue that the inference is unreasonable. Govt. Reply at 7. Accordingly, the inference must be drawn in plaintiffs' favor, and considered with the NSA Letter's direct evidence of AT&T's and Verizon's participation.

Instead of arguing that the inference is unreasonable, the government relies on *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015). That case provides no support for the government's position because plaintiffs' evidence in this case is much broader and more developed than the evidence before the *Klayman* court. That lawsuit involved only Verizon Wireless and, unlike here, the record contained no direct evidence from the government that Verizon Wireless participated in

---

[1] AT&T Inc.'s SEC Form 8-K, at 2-3 (July 24, 2018), *available at* https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/quarterly-earnings/2018/2q-2018/Form 8-K.pdf. Plaintiffs request the Court judicially notice this document.

[2] Verizon Communications Inc.'s SEC Form 10-Q, at 39, 42 (July 31, 2018), *available at* https://www.sec.gov/Archives/edgar/data/732712/000073271218000044/a2018q210-q.htm. Plaintiffs request the Court judicially notice this document.

[3] The government makes a silly objection to plaintiffs' citation to a learned treatise for the fact that a phone call between customers of two different phone companies generates two phone records—one held by each phone company. George Molczan, *A Legal And Law Enforcement Guide To Telephony*, pp. 34, 38 (2005) (ECF No. 417-4, Ex. F). The fact is a basic one not subject to reasonable dispute—and not disputed by the government—and easily "'could be presented in an admissible form at trial.'" *Fonseca*, 374 F.3d at 846. Moreover, plaintiffs request that the Court take judicial notice of this fact, which "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b)(2).

the phone records program. *Klayman* also did not consider whether exclusion of both AT&T and Verizon from the program would have left the government still able to perform three-hop searches yielding the phone records of 120 million persons. For no plaintiff to have standing here, *both* AT&T and Verizon would have had to have been excluded from the program. *Klayman* also ignored the PCLOB disclosures about the phone records program's scope. And the support *Klayman* sought to draw from *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), is unavailing here because what *Clapper* addressed was the likelihood that a person would be *targeted* for surveillance, not the likelihood that untargeted persons would be swept up in a mass surveillance collection of all the call records of major telephone companies, resulting in "'comprehensive' analysis of telephone communications 'that cross different providers and telecommunications networks.'" PCLOB 215 Report at 22.

### B. Plaintiffs Have Standing To Challenge The Government's Interference With Their Internet Communications

#### 1. Plaintiffs' Evidence Of The Government's Interference With Their Internet Communications Is Competent And Admissible

The government admits that plaintiffs' evidence shows that the splitters copy all of the traffic passing over AT&T's peering links and that at least one of each plaintiff's communications has passed over those peering links since 2001. Govt. Reply at 13:10-15. But it challenges the evidence showing AT&T's participation in the NSA's Internet content surveillance, and the presence of surveillance equipment in AT&T's facilities.

##### (a) The AT&T Documents Attached To The Klein Declaration Are Authentic

[redacted]

[redacted]

Klein's testimony, as an AT&T employee who used the documents in the course of his employment, also authenticates those documents. ECF No. 84-2 (Klein Decl.), ¶¶ 15, 19-20, 22, 25-31, 34-36. Klein was responsible for maintaining the fiber-optic cables connecting the splitters to the equipment in the AT&T secure room and for connecting new cables, and he relied upon the AT&T documents to perform that task. *Id.*

**(b) Evidence Regarding The Search Devices In The AT&T Secure Room Is Admissible**

[redacted]

[redacted]

Even without Russell's testimony, the AT&T documents and the evidence they contain about the surveillance devices in the AT&T secure room would be admissible on several independent grounds.

First, they are admissible under Fed. R. Evid. 801(d)(2)(D) as statements by AT&T as the government's agent in conducting surveillance. The PCLOB makes clear that telecommunications providers like AT&T conduct Internet backbone surveillance as agents of the government: The NSA's surveillance occurs "with the compelled assistance of providers that control the telecommunications 'backbone' over which . . . Internet communications transit." ECF No. 417-2, Ex. B ("PCLOB Section 702 Report at 7"). "The provider is compelled to assist the government in acquiring communications across these circuits." *Id*. at 37. These acquisitions are conducted using "NSA-designed upstream Internet collection devices." *Id*. at 39. And the evidence of the NSA's involvement discussed in the next section below shows the NSA's connection to the surveillance devices and facilities discussed in the AT&T documents. The AT&T documents thus concern matters within the scope of AT&T's assistance to the government in conducting surveillance and made during the existence of that relationship. The government's classified responses to Plaintiffs' Requests For Admission Nos. 52-61, if forthright and not evasive, should also establish that the documents evidence AT&T's participation in the government's Internet backbone surveillance.

Second, the AT&T documents are admissible as AT&T business records. Fed. R. Evid. 803(6). Rule 803(6) includes not only records of "acts" but also "events" and "conditions" (two

categories omitted by the government, Govt. Reply at 16); this language easily encompasses AT&T's implementation and operation of a surveillance facility on behalf of the government. And despite the government's unsupported protestations, operating surveillance devices on behalf of the government is a regularly conducted activity of AT&T, as AT&T's transparency reports demonstrate. ECF No. 417-4, Ex. C. Because these surveillance devices are integrated into it AT&T's Internet backbone, they are integrated into its other regularly conducted activities; it is crucially important that they operate in harmony with the rest of AT&T's network and not disrupt Internet transmissions. Marcus Decl. ¶¶ 34, 60, 62, 116; ECF No. 417-6 (Reid Decl.), ¶¶ 22, 53-57, 63-64; ECF No. 417-7 (Blaze Decl.), ¶¶ 38, 56.

Finally, the government contends the documents are inadmissible hearsay because they are only a statement of plan or intent. This ignores Russell's independent testimony and the hearsay exceptions for business records and statements of an agent. Even apart from those, the government is wrong because statements of plan or intent are admissible to show the declarant thereafter acted in accordance with the stated intent. Fed. R. Evid. 803(3) (statements reflecting plan or intent are admissible); *U.S. v. Best*, 219 F.3d 192, 198 (2d Cir. 2000) (statement of plan or intent can be used to "prove that the declarant thereafter acted in accordance with the stated intent"); *U.S. v. Donley*, 878 F.2d 735, 737-38 (3d Cir. 1989) (same); *U.S. v. Astorga-Torres*, 682 F.2d 1331, 1335 (9th Cir. 1982) (same). So even if the AT&T documents were only future plans for surveillance devices, they are admissible to show AT&T thereafter installed and operated those devices as the documents reflect.

**(c) Evidence Regarding The NSA's Involvement Is Admissible**

Nor is there any doubt that the Internet backbone surveillance of plaintiffs' communications occurs at the government's direction. The PCLOB Section 702 Report, quoted above, is clear about the government's direction and control of providers in conducting Internet backbone surveillance. The ultimate determination of whether the government is liable for AT&T's compelled assistance is, of course, a merits determination, not a standing issue.

Klein's testimony of the NSA's involvement in the AT&T secure room at his workplace is based on his personal observations and experiences on the job. *Barthelemy v. Air Lines Pilots*

*Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990) ("personal knowledge and competence to testify are reasonably inferred from [employees'] positions and the nature of their participation in the matters to which they swore"). It is no different than any other testimony by an employee regarding his on-the-job experiences, his observations of co-workers, his company's policies and practices, or its interactions with another entity.

Employees may testify about the functions and activities of others within the organization that employs them and about the relationship between the organization and outside entities, including government entities; such testimony is not hearsay because it is based on personal, on-the-job observations. *U.S. v. Neal*, 36 F.3d 1190, 1206 (1st Cir. 1994); *Great American Assur. Co. v. Liberty Surplus Ins. Corp.*, 669 F. Supp. 2d 1084, 1089 (N.D. Cal. 2009) (employee can testify to company policies based on her "experience and perceptions" on the job); *Sjoblom v. Charter Comms.*, 571 F. Supp. 2d 961, 968-69 (W.D. Wis. 2008) (employees may testify about the activities of their supervisors and co-workers that they observe).[4] Moreover, an employee's "[p]ersonal knowledge can include 'inferences and opinions, so long as they are grounded in personal observation and experience.'" *Neal*, 36 F.3d at 1206; *see also* Fed. R. Evid. 701 (lay opinion admissible).

For instance, in *Neal*, a bank employee testified to information she learned in the course of her job, including the status of the bank's relationship with a federal agency (the Federal Deposit Insurance Corporation (FDIC)) and the states where the bank's customers were located, even

[4] *Accord U.S. v. Famania-Roche*, 537 F.3d 71, 76 (1st Cir. 2008) (low-level drug dealer could testify to activities and drug sales by other drug dealers in narcotics organization she was part of); *DIRECTV, Inc. v. Budden*, 420 F.3d 521, 529 (5th Cir. 2005) (employee could testify about facts concerning another company he learned through a law enforcement investigation); *U.S. v. Doe*, 960 F.2d 221, 223 (1st Cir. 1992) (gun shop owner could testify that pistol sold to him by another United States company was manufactured in Brazil); *White v. MPW Indus. Servs., Inc.*, 236 F.R.D. 363, 369 (E.D. Tenn. 2006) ("employees . . . would have learned during the normal course of their employment how the company operates and what the company's policies were"); *U.S. v. Wirtz*, 357 F. Supp. 2d 1164, 1169-70 (D. Minn. 2005) (employee could testify that employees of a different company provided certain information and documents to his company even though he had no personal contact with the employees of the other company). "Generally, employees have personal knowledge to testify about their experiences at their place of employment." *In re Hilton*, 544 B.R. 1, 8 (Bankr. N.D.N.Y. 2016).

though her knowledge was based solely on hearsay statements in documents she reviewed. 36 F.3d at 1206.

Thus, Klein is competent to testify about his personal knowledge and observations on the job regarding AT&T's relationship with the NSA. This evidence includes the following: Klein, who otherwise had keys and free access to all parts of AT&T's Folsom Street Facility, has personal knowledge that the reason he was excluded only from the AT&T secure room is because AT&T's policy was to restrict access to only persons cleared by the NSA, even in emergencies. Klein Decl. ¶¶ 17, 18. AT&T employee Philip Long confirms that AT&T restricted access to the secure room. ECF No. 417-5 (Long Decl.), ¶ 21. Likewise, Klein testified from his personal knowledge about visiting the AT&T secure room while it was under construction (where he saw AT&T employee "FSS #2," whom Klein had observed meeting with an NSA agent and whom Klein knew to be in charge of the room, installing equipment) and of again entering the AT&T secure room after it was in operation. *Id*. at ¶¶ 10, 12, 14, 17. And Klein's statements that "The NSA agent came and met with FSS #2" and "The NSA agent did come and speak to [AT&T employee] FSS #1" are also direct personal observations, not hearsay. *Id*. at ¶¶ 10, 16.

In addition to Klein's admissible observations of the NSA's involvement, the statements made to Klein by AT&T's management and his co-workers about the NSA's activities and NSA's connection to the AT&T secure room are admissible. Klein Decl. ¶¶ 10, 16. They are admissible under *Neal* as knowledge learned by Klein on the job, just as the witness in *Neal* learned about her employer's relationship with the FDIC. They are also independently admissible nonhearsay because AT&T is the agent of the government in assisting the government in electronic surveillance, as discussed above, and statements by an agent on a matter within the scope of the agency are admissible nonhearsay. Fed. R. Evid. 801(d)(2)(D). Similarly admissible are the statements by Klein's co-worker that other splitter cabinets exist at AT&T facilities in Seattle, San Jose, Los Angeles, and San Diego. Klein Decl. ¶ 36.

The e-mail to Klein from AT&T management regarding the NSA and the statements to Klein by his manager and a co-worker telling of upcoming visits by an NSA agent (Klein Decl. ¶¶ 10, 14, 16) are independently admissible under Federal Rule of Evidence 803(3) as statements

of future intention to meet with the NSA, that the intended purpose of the first meeting was that "the NSA agent was to interview FSS #2 for a special job" managing the AT&T secure room, that the intended purpose of the second meeting was to discuss "FSS #3's suitability to perform the special job that FSS #2 had been doing," and that AT&T's management's plan and intent was to cooperate with the NSA. Further, they are also evidence that AT&T employees actually met with NSA agents and managed the AT&T secure room to facilitate the NSA's purposes, and that AT&T did cooperate with the NSA. *Best*, 219 F.3d at 198 (statement of plan or intent can be used to "prove that the declarant thereafter acted in accordance with the stated intent"); *Donley*, 878 F.2d at 737-38; *Astorga-Torres*, 682 F.2d at 1335.

**2. Who Holds The Keys To The AT&T Secure Room Is Irrelevant To Plaintiffs' Standing**

The government erroneously contends that it is essential to plaintiffs' standing that they show that the NSA controls the operation of the AT&T secure room. Govt. Reply at 16. Apparently, the government is relying on some secret argument that it is not liable because AT&T operates the equipment that performs the surveillance the NSA orders.

But that's a red herring. All that matters is that the surveillance can be "fairly trace[d]" to the government. *Jewel v. NSA*, 673 F.3d 902, 912 (9th Cir. 2011). Although the fact of the government's control of the AT&T secure room is well supported by the evidence just recited, it is not a fact essential to plaintiffs' standing. Plaintiffs' standing does not depend on who has day-to-day physical control of the spaces containing the various devices used to conduct surveillance of AT&T's Internet backbone, or who has the key to the door of those locations, or who approves those who are permitted inside.

The government's suggestion that it is not liable for actions taken by AT&T in furtherance of the government's surveillance programs is wrong on many counts. It is wrong because standing does not require the government to be the immediate cause of plaintiffs' injuries-in-fact, only that those injuries be "fairly traceable" to the government's challenged conduct. It is wrong because the Ninth Circuit has already ruled that "the harms Jewel alleges are 'fairly traceable to the challenged action' of the NSA. . . . [T]he harms Jewel alleges—invasion of privacy and violation

of statutory protections—can be directly linked to this acknowledged surveillance program." *Jewel*, 673 F.3d at 912. It is wrong because the PCLOB has found that the actions telecommunications providers take in conducting Internet backbone surveillance are compelled by the government. And it is wrong because plaintiffs have shown that the NSA does control access to the AT&T secure room, and that only AT&T personnel who have been cleared by the NSA are permitted into the room.

As plaintiffs explained in their opening brief, they need only prove it is more likely than not—and not any greater degree of certainty—that they have suffered an injury-in-fact. *Lujan Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Plaintiffs have done so. Plaintiffs' evidence establishes the AT&T secure room receives communications from AT&T's Internet backbone, identifies the spy devices found in the secure room, and its connection to the NSA. If the government's secret evidence tells a different story, that is a factual dispute precluding any grant of summary judgment.

**3. Plaintiffs' Standing Does Not Turn On The Particular Technical Mechanism The Government Has Used To Interfere With Their Communications**

While the Klein evidence and the independent opinions of the four experts who analyze it is sufficient to establish plaintiffs' standing to challenge the government's interference with their Internet communications, plaintiffs' standing does not turn on the particular devices or methods that the government has chosen to use to conduct its surveillance.

Given the government's focus on "copying" and its suggestion that plaintiffs are mistaken about whether or how their communications are copied (Govt. Reply at 12, 17), plaintiffs surmise that the government has a secret theory of nonliability that it has deployed in its classified submissions. It may be that the government contends that no copying occurs at all, but if so that would just be a factual dispute precluding summary judgment. As plaintiffs' experts have explained, intercepting, filtering, and selecting communications from the Internet backbone based on their email addresses requires some form of copying and reassembly of the email message. Reid Decl. ¶¶ 22(c), 59-61; Blaze Decl. ¶¶ 12, 22, 27, 33, 38; *see Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (Wiretap Act violated if communications are "'captured or redirected in any

way'").

It may be that the government secretly defines "copying" to exclude the copying shown by plaintiffs' evidence, but that, too, would present a merits question regarding whether the copying shown by plaintiffs' evidence is a Wiretap Act violation. *Jewel*, 673 F.3d at 911 n.5.

Or it may be that the government contends that it is not legally liable for any actions taken by AT&T as part of conducting Internet backbone surveillance. But whether the government is liable for actions taken by AT&T is a merits question, not a standing question, and the Court may not broach it on summary judgment. *Jewel*, 673 F.3d at 907 n.4, 911 n.5. Any such contention that the government is not liable would also present a factual dispute as to the exact nature of the government's involvement in AT&T's actions, barring summary judgment.

**4. Evidence Must Be Viewed In The Light Most Favorable To Plaintiffs**

Plaintiffs' account of how Internet backbone surveillance occurs relies not just on Klein's account and the testimony of the four experts, but also on other sources like the PCLOB 702 Report, which dovetails with plaintiffs' other evidence. In a telling example of how the government reads evidence in the light most favorable to itself, rather than to plaintiffs, it contests the import of statements made by the PCLOB describing the "intercept[ion of] communications directly from the Internet backbone" (PCLOB 702 Report at 124) that support plaintiffs' standing. Govt. Reply at 17-18. But weighing and evaluating those statements is a question for the trier of fact. Contesting the import of those statements at most creates a dispute of fact precluding summary judgment. Similarly, any secret argument regarding "copying" or the mechanism of Internet backbone surveillance is also likely to involve the government improperly presenting evidence in the light most favorable to itself, rather than to plaintiffs.

**5. The Additional Evidence Plaintiffs Rely On Is Also Admissible**

The NSA Draft OIG Report is yet further evidence showing AT&T's and Verizon's participation in Internet backbone surveillance. ECF No. 417 at 9 n.6, 15; ECF No. 147, Ex. A at 27-29, 33-34. It also evidences AT&T's and Verizon's participation in the phone records program and the Internet metadata program. ECF No. 417 at 9 & n.6, 19-20. The government disputes the authenticity of the NSA Draft OIG Report. It is undisputed that the NSA Inspector General

prepared a report on the President's Surveillance Program. ECF No. 35 at Preface, 2-3. And the Court knows the NSA Draft OIG report is authentic from the government's classified response to Plaintiffs' Request For Admission No. 50. It is also authenticated by Edward Snowden. Snowden Decl. ¶¶ 2-5.

The government also improperly discounts the declaration of Ashkan Soltani, arguing that it is insufficient by itself to establish standing and that it does not specify where NSA's Internet backbone surveillance devices are located. Govt. Reply at 18 n.10. But that both erroneously considers the declaration in isolation from the rest of the evidence and misses Soltani's point: Email providers like Gmail and Yahoo (which supplies the AT&T-branded email services used by AT&T's customers, ECF Nos. 417-12 at ¶ 14; 417-13 at ¶ 15) are constantly shipping customer emails over the Internet between their data centers (both within the U.S. and abroad) in a process that is completely independent of whether the customer is sending an email or where the customer is located. ECF No. 417-8 (Soltani Decl.) at ¶¶ 2, 16-18, 21-25. Because these shipments are constantly traversing the Internet, the NSA's Internet backbone interception devices are likely to encounter these email shipments regardless of where these devices are located. *Id*. at ¶¶ 16, 25.

### C. Plaintiffs Have Standing To Challenge The Government's Collection Of Internet Metadata

Plaintiffs' brief at pages 19-21 lays out the evidence showing that the Internet metadata collection program was "massive" and "wholly non-targeted bulk production," and was not limited to "streams of data with a relatively high concentration of Foreign Power communications." PR/TT Order at 115, 74. Plaintiffs explain how not only was the authorized collection intended to be massive and untargeted, but that NSA "continuously" and "systemic[ly]" exceeded the scope of what the FISC authorized it to collect, resulting in "sweeping and non-targeted" overcollection. PR/TT Order at 3, 20, 110.

Having destroyed during the pendency of this litigation all of the Internet metadata it collected after July 2004, the government reprises its refrain that all of plaintiffs' many thousands of Internet communications may have magically escaped the government's dragnet, and that plaintiffs cannot prove otherwise. In the government's view, no matter how broad a mass

surveillance program is, there is no standing unless the plaintiff can identify a specific communication or record that the program collected, and thus no standing when the government destroys what it has collected.

But that is not the law. Plaintiffs need only prove it is more likely than not that over the years at least one of their communications had its Internet metadata collected. The size and untargeted nature of the program, with both its massive scope and its even broader overcollection, is sufficient to demonstrate standing.

Indeed, the indeterminate, ever-changing, and essentially random nature of Internet communications routing means that wherever on the Internet backbone the Internet metadata collection devices may have been located, over the years it is more probable than not that at least one of each plaintiffs' communications passed through it. Reid Decl. ¶¶ 21, 23, 26-30, 34-36, 48-57, 62-64; Blaze Decl. ¶¶ 15, 21, 26, 40, 42-43.

In addition, the NSA OIG Draft Report, discussed above, confirms AT&T and Verizon's participation in the Internet metadata program. ECF No. 147, Ex. A at 27-29, 34.

Finally, it is possible that the surveillance devices at AT&T's Folsom Street facility, and whatever other devices the NSA has used for Internet backbone surveillance, were also used to collect Internet metadata. As plaintiffs' experts explain, in order to collect the "to" and "from" email addresses that the government characterizes as "metadata," it is necessary to reconstruct and examine the content of the email message. Reid Decl. ¶¶ 22(c), 59-61; Blaze Decl. ¶¶ 12, 22, 27, 33, 38. So any Internet metadata collection program is necessarily copying, at least temporarily, and examining the content of the emails whose metadata it is collecting. If the Internet backbone surveillance devices at AT&T's Folsom Street facility and elsewhere were used to collect Internet metadata as well, then the same evidence that shows plaintiffs' standing to challenge Internet content surveillance also gives them standing to challenge Internet metadata collection.

## II. The State Secrets Privilege Is No Barrier To Either This Court's Determination Of Standing Or To Moving Forward Using Classified Evidence Ex Parte And In Camera To Decide The Merits

Before the Court are two questions regarding the state secrets privilege and the two statutes the Court has held preempt it, 50 U.S.C. § 1806(f) and 18 U.S.C. § 2712(b)(4). The answers to

these questions are straightforward, despite the convoluted arguments raised by the government.

The first question is whether in the post-standing, merits phase of this litigation the Court should use classified evidence reviewed *ex parte* and *in camera* to decide the merits rather than applying the state secrets privilege. The answer is "Yes." The Court has already granted summary judgment to plaintiffs holding that sections 1806(f) and 2712(b)(4) preempt the state secrets privilege. And the Ninth Circuit has held en banc that the state secrets privilege does not apply when Congress enacts procedures for using classified evidence like section 1806(f). *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1092 & n.15 (9th Cir. 2010) (en banc).

The second question is whether the Court should also use the classified evidence in deciding plaintiffs' standing. It should do so because plaintiffs have met any possible threshold test for using the classified evidence. However, the public evidence alone is sufficient to show plaintiffs' standing, and if the Court agrees then it need not reach the question of whether to consider the classified evidence as well.

### A. The Court Must Use The Classified Evidence In Deciding The Merits

#### 1. The Court's Prior Rulings And The Ninth Circuit's *Mohamed* Opinion Require The Court To Decide The Merits Using The Classified Evidence

In granting partial summary judgment to plaintiffs in 2013, the Court squarely, and correctly, held that Congress preempted the state secrets privilege with section 1806(f) and section 2712(b)(4).[5] *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1097, 1103, 1104-05, 1112 (N.D. Cal. 2013). Since then, the Court has twice reiterated that holding. ECF Nos. 347 at 1-2; 340 at 2.

Expressly citing section 1806(f), the Ninth Circuit in *Mohamed* similarly held that the "judge-made" states secrets doctrine must yield when Congress exercises its "authority to enact remedial legislation authorizing appropriate causes of action and procedures to address claims" that would otherwise be barred by the state secrets privilege. 614 F.3d at 1092 & n.15.

Thus, as the Court has held, "the *in camera* review procedure in FISA applies and preempts

[5] The government makes the odd and unsupported argument that plaintiffs have abandoned section 1806(f) and rely only on section 2712(b)(4). Govt. Reply at 26. That is erroneous. Plaintiffs rely on both statutes; Congress designed them to work in tandem and plaintiffs are entitled to use both.

the determination of evidentiary preclusion under the state secrets doctrine." *Jewel*, 965 F. Supp. 2d at 1104. In post-standing proceedings on the merits, the Court therefore must review the classified evidence *in camera* and *ex parte* and use that classified evidence to decide the merits.

The government argues that section 1806(f) and section 2712(b)(4) do not preempt the state secrets privilege, but it presents no grounds justifying reconsideration by the Court of its 2013 ruling that those statutes preempt the privilege. Govt. Opening Br. at 23; Govt. Reply at 27. Instead, it ignores the Court's ruling and pretends that the Court has never ruled on the preemption issue. (Previously, the government freely admitted that "[t]he Court . . . held that section 1806(f) preempts application of the state secrets privilege in these cases." ECF No. 167 at 4; *see id*. at 6-7.) The government likewise ignores the Ninth Circuit's conclusion in *Mohamed* that when Congress enacts statutory schemes like section 1806(f), it preempts the state secrets privilege.

But this Court's rulings, and those of the Ninth Circuit, may not be evaded simply by ignoring them. Those rulings remain correct for all of the reasons previously stated by the Court and all of the reasons plaintiffs have presented. *See Jewel*, 965 F. Supp. 2d at 1097, 1103-05, 1112; ECF Nos. 417 at 28-29; 407 at 4-5; 140 at 4-7; 112 at 2-13; 83 at 12-22.

**2. Plaintiffs Meet Any Standard For Using Sections 2712(b)(4) Or 1806(f)**

As plaintiffs' opening brief explains, plaintiffs meet any standard for using section 2712(b)(4) or section 1806(f), including the "aggrieved person" standard. ECF 417 at 23-28.

Plaintiffs meet the "aggrieved person" standard adopted by this Court in the related *In re NSA* multidistrict litigation because their "allegations 'are sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.'" *In re NSA Telecom. Records Litigation*, 595 F. Supp. 2d at 1085.

Plaintiffs meet the *Wikimedia* aggrieved-person standard because they have "adduce[d] evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance." *Wikimedia*, 2018 WL 3973016, at *8.

Plaintiffs meet the government's aggrieved-person test because they have shown that their Internet communications have been subjected to electronic surveillance and that their phone records and Internet metadata have been collected by the government.

Plaintiffs are aggrieved persons under the "zone of interests" test because they come within the zone of interests of the Wiretap Act, the SCA, and section 2712. *Dir., Office of Workers' Comp. Prog. v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 127 (1995); *Jewel*, 673 F.3d at 913.

**3. Section 2712, Including Section 2712(b)(4), Applies To Plaintiffs' Claims**

The government makes the strange argument that the section 2712 cause of action is limited to claims of "malicious leaks," that plaintiffs' claims are not malicious-leak claims, and that therefore section 2712(b)(4) does not apply to plaintiffs' claims. Govt. Reply at 28.

This argument is foreclosed by the Court's prior rulings. The Court has ruled that, as the plain language of the statute provides, section 2712(b)(4) displaces the state secrets privilege and governs the use of classified evidence for claims brought under section 2712. *Jewel*, 965 F. Supp. 2d at 1104-05, 1112; ECF No. 347 at 1-2; ECF No. 340 at 2.

The Court has also rejected the government's argument that section 2712 is limited to malicious-leak claims. The Court held that section 2712's cause of action encompasses plaintiffs' claims because it applies to any violation of the Wiretap Act or the SCA, not just claims for the unlawful use or disclosure of communications or communications records: "The plain language of Section 2712(a) does not limit the waiver of sovereign immunity for damage claims under the SCA and the Wiretap Act to claims for the use and disclosure of information." *Jewel*, 965 F. Supp. 2d at 1107. The Ninth Circuit also held that plaintiffs' statutory claims are proper. *Jewel*, 673 F.3d at 913.

Even if the issue of section 2712's scope were not foreclosed, the government's argument would lack merit. The government relies on a snippet from a single senator to argue that section 2712 is limited to claims of malicious leaks. Govt. Reply at 28. The government badly misstated the legislative history of section 2712 in the proceedings leading up to the Court's 2013 order. ECF No. 140 at 6-7 & n.3 (explaining section 2712's legislative history); ECF No. 133 (12/14/12 RT) at 106-107. The government again gets it wrong. While section 2712 certainly encompasses malicious leaks, nothing in the senator's statement suggests the statute is limited to leaks. The statement focuses on liability for leaks because that liability was newly created in section 2712,

while liability for Wiretap Act and SCA violations had existed previously in 18 U.S.C. § 2520 and 18 U.S.C. § 2707 and was merely being transferred to section 2712 by the USA PATRIOT Act.

The government's related argument that even if section 2712(b)(4) applies, it gives a court discretion not to use the classified evidence to decide the issues before it also fails. Govt. Reply at 27. This argument rests on the use of the word "may" in the phrase "Notwithstanding any other provision of law, the procedures set forth in section [1806(f)] . . . shall be the exclusive means by which materials governed by those sections may be reviewed." 18 U.S.C. § 2712(b)(4). But saying that procedure X is the only procedure by which one class of evidence may be used does not authorize a court to refuse altogether to use the evidence. Section 2712(b)(4) incorporates the procedures of section 1806(f), and the "shall" the government is looking for is in section 1806(f): "the United States district court . . . *shall*, notwithstanding any other law, . . . review in camera and ex parte" the classified evidence. 50 U.S.C. § 1806(f) (italics added).

Finally, the government argues that plaintiffs can never be aggrieved persons under section 2712 because 18 U.S.C. § 2510(11) links *its* definition of "aggrieved person" to the interception of communications. Govt. Reply at 29-31. But the government ignores that section 2712, including section 2712(b)(4) and its incorporation of section 1806(f)'s procedures, applies to "[a]ny person who is aggrieved by any willful violation of this chapter [the SCA] or of chapter 119 [the Wiretap Act]"—a provision that extends beyond communications interceptions under the Wiretap Act to encompass communications records violations under the SCA. 18 U.S.C. § 2712(a). Plaintiffs' claims thus are within the scope of sections 2712(a) and 2712(b)(4), as the Court has held.

The government further argues that copying and redirecting of a communication is never a Wiretap Act violation, and so plaintiffs cannot be aggrieved. Govt. Reply at 30. The argument is wrong because the Wiretap Act is violated if communications are "'captured or redirected in any way.'" *Noel*, 568 F.3d at 749. The argument also improperly conflates the merits of whether the government has violated the Wiretap Act with the threshold question of whether Congress has directed the Court to use classified evidence to decide the merits. If the government were correct that a party must win on the merits before the Court can use section 1806(f)'s procedures to decide the merits, those procedures would never come into play.

**B. The Court Should Use The Classified Evidence At The Standing Phase As Well**

In addition to using the classified evidence to decide the merits in the post-standing phase, the Court should use it to decide standing as well. (If the Court determines that plaintiffs' public evidence alone establishes their standing, then it need not reach this question.)

As plaintiffs' opening brief explains, section 2712(b)(4) extends the scope of section 1806(f) to encompass not only merits determinations but any other determination, including standing. ECF 417 at 23-24. And as explained in plaintiffs' opening brief and above, plaintiffs have met any test for using sections 2712(b)(4) and 1806(f), including showing they are aggrieved persons. ECF 417 at 24-28.

**C. Litigating Standing Does Not Require Public Disclosure Of Classified Evidence**

The government contends that litigating standing would result in the disclosure of additional reams of secret evidence. Govt. Reply at 19-22. This argument lacks merit.

First, if the government has obeyed the Court's order to "marshal all the evidence" relevant to standing, then the Court already possesses all the classified evidence relevant to standing and there is no additional evidence. The government is not put to the choice of either presenting classified evidence or remaining silent (Govt. Reply at 20); it has already presented that evidence.

Second, the government is wrong to assert that there is no way for it to rely on the classified evidence at a bench trial (which this will be, per 18 U.S.C. § 2712(b)(3)) without publicly disclosing it. Congress addressed this dilemma by enacting section 1806(f) and section 2712(b)(4). Under those provisions, the Court is to use the classified evidence without making any disclosure of it, as Congress intended. If it finds after weighing all the evidence that plaintiffs lack standing, it can issue a public judgment dismissing plaintiffs' claims, but disclosing nothing about the classified evidence or saying anything about any classified reasons why plaintiffs lack standing. It can present its reasoning in a classified opinion. *See Ibrahim v. Dep't of Homeland Security*, No. 06-cv-0545-WHA (N.D. Cal.), ECF Nos. 652, 683, 684, 686 (discussing procedures for preparing and filing classified opinion after a civil trial involving classified evidence).

If instead it finds that plaintiffs have standing, it need not issue any opinion at all at that time, but can proceed to the post-standing merits phase.

Indeed, if the government's classified evidence creates a factual dispute as to plaintiffs' standing, the disputed facts doubtless are ones that go to the merits as well as to standing (e.g., the methods and devices used to conduct Internet backbone surveillance) and the proper course is *not* to issue a separate ruling on standing but instead to try the merits. When "the jurisdictional issue and substantive claims are so intertwined that resolution of the jurisdictional question is dependent on factual issues going to the merits," then "the intertwined jurisdictional facts *must* be resolved *at trial* by the trier of fact." *Rosales v. U.S.*, 824 F.2d 799, 803 (9th Cir. 1987) (italics added).

The trial would consist of plaintiffs presenting their evidence publicly, the government presenting any unclassified evidence it has publicly, and the Court considering the classified evidence *in camera* and *ex parte*. At the conclusion of the trial, if plaintiffs' claims lack merit, the Court can enter judgment for the government with a classified opinion, and plaintiffs and the public will be none the wiser as to the identities of the telecommunications providers participating in the surveillance programs, the identities of surveillance targets, the locations of the surveillance, the methods by which the surveillance is conducted, or any other secret fact. If instead the Court finds plaintiffs have proven their communications and communications records have been subjected to unlawful surveillance, then the Court can enter judgment for plaintiffs with a classified opinion to the extent classification is lawful and justified. That is what Congress has required of the Court by creating the section 2712 cause of action and the procedures for litigating that cause of action with classified evidence.

## CONCLUSION

The government's summary judgment motion should be denied and the Court should order that the case proceed to discovery on the merits and trial, using classified evidence reviewed *ex parte* and *in camera* to decide the issues.

DATE: November 2, 2018

Respectfully submitted,

*s/Richard R. Wiebe*
RICHARD R. WIEBE

CINDY COHN
DAVID GREENE
LEE TIEN

KURT OPSAHL
JAMES S. TYRE
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKEY
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
ROYSE LAW FIRM, PC

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
PHILIP J. TASSIN
KEKER, VAN NEST & PETERS LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs