

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION..... 1

ARGUMENT 3

I. Plaintiffs Have Proffered Sufficient Public Evidence Of Their Standing To Defeat Summary Judgment And To Proceed To The Merits Using Classified Evidence 3

 A. Plaintiffs Have Standing To Challenge The Collection Of Their Phone Records 4

 B. Plaintiffs Have Standing To Challenge The Government’s Interference With Their Internet Communications..... 7

 1. Plaintiffs’ Evidence Of The Government’s Interference With Their Internet Communications Is Competent And Admissible..... 7

 2. Who Holds The Keys To The AT&T Secure Room Is Irrelevant To Plaintiffs’ Standing..... 13

 3. Plaintiffs’ Standing Does Not Turn On The Particular Technical Mechanism The Government Has Used To Interfere With Their Communications..... 14

 4. Evidence Must Be Viewed In The Light Most Favorable To Plaintiffs..... 15

 5. The Additional Evidence Plaintiffs Rely On Is Also Admissible 15

 C. Plaintiffs Have Standing To Challenge The Government’s Collection Of Internet Metadata 16

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 17

 A. The Court Must Use The Classified Evidence In Deciding The Merits..... 18

 1. The Court’s Prior Rulings And The Ninth Circuit’s *Mohamed* Opinion Require The Court To Decide The Merits Using The Classified Evidence 18

 2. Plaintiffs Meet Any Standard For Using Sections 2712(b)(4) Or 1806(f)..... 19

 3. Section 2712, Including Section 2712(b)(4), Applies To Plaintiffs’ Claims 20

 B. The Court Should Use The Classified Evidence At The Standing Phase As Well 22

 C. Litigating Standing Does Not Require Public Disclosure Of Classified Evidence 22

CONCLUSION 23

TABLE OF AUTHORITIES

Cases

Barthelemy v. Air Lines Pilots Ass’n,
897 F.2d 999 (9th Cir. 1990)..... 10, 11

Clapper v. Amnesty Int’l USA,
568 U.S. 398 (2013) 7

Dir., Office of Workers’ Comp. Prog. v. Newport News Shipbuilding & Dry Dock Co.,
514 U.S. 122 (1995) 20

DIRECTV, Inc. v. Budden,
420 F.3d 521 (5th Cir. 2005)..... 11

Fonseca v. Sysco Food Servs. of Arizona, Inc.,
374 F.3d 840 (9th Cir. 2004)..... 4, 6

Fraser v. Goodale,
342 F.3d 1032 (9th Cir. 2003)..... 4

Great American Assur. Co. v. Liberty Surplus Ins. Corp.,
669 F. Supp. 2d 1084 (N.D. Cal. 2009)..... 11

Hepting v. AT&T,
No. 06-cv-0672 (N.D. Cal.)..... 7

Ibrahim v. Dept. of Homeland Security,
No. 06-cv-0545-WHA (N.D. Cal.)..... 22

In re NSA Telecom. Records Litigation,
595 F. Supp. 2d 1077 (N.D. Cal. 2009)..... 3, 19

Jewel v. NSA,
2015 WL 545925 (N.D. Cal. Feb. 10, 2015)..... 5

Jewel v. NSA,
673 F.3d 9022 (9th Cir. 2011)..... 13, 14, 15, 20

Jewel v. NSA,
965 F. Supp. 2d 1090 (N.D. Cal. 2013)..... 18, 19, 20

Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 14

Mohamed v. Jeppesen Dataplan, Inc.,
614 F.3d 1070 (9th Cir. 2010) (en banc)..... 18, 19

New York Times v. NSA,
No. 15-cv-2383 (S.D.N.Y.) 4

Noel v. Hall,
568 F.3d 743 (9th Cir. 2009)..... 14

1 *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015)..... 6, 7

2 *Orr v. Bank of America*,

3 285 F.3d 764 (9th Cir. 2002)..... 5

4 *Pavoni v. Chrysler Group*,

5 789 F.3d 1095 (9th Cir. 2015)..... 4

6 *Rosales v. U.S.*,

7 824 F.2d 799, 803 (9th Cir. 1987)..... 23

8 *Sjoblom v. Charter Comms.*,

9 571 F. Supp. 2d 961 (W.D. Wis. 2008)..... 11

10 *U.S. v. Astorga-Torres*,

11 682 F.2d 1331 (9th Cir. 1982)..... 10, 13

12 *U.S. v. Best*,

13 219 F.3d 192 (2d Cir. 2000)..... 10, 13

14 *U.S. v. Dhinsa*,

15 243 F.3d 635 (2d Cir. 2001)..... 5

16 *U.S. v. Doe*,

17 960 F.2d 221 (1st Cir. 1992)..... 11

18 *U.S. v. Donley*,

19 878 F.2d 735 (3d Cir. 1989)..... 10, 13

20 *U.S. v. Famania-Roche*,

21 537 F.3d 71 (1st Cir. 2008)..... 11

22 *U.S. v. Neal*,

23 36 F.3d 1190 (1st Cir. 1994)..... 11, 12

24 *U.S. v. Wirtz*,

25 357 F. Supp. 2d 1164 (D. Minn. 2005)..... 11

26 *White v. MPW Indus. Servs., Inc.*,

27 236 F.R.D. 363 (E.D. Tenn. 2006)..... 11

28 *Wikimedia Found. v. NSA/CSS*, 2018 WL 3973016,

(D. Md. Aug. 20, 2018)..... 3, 19

Statutes

18 U.S.C. § 2510(11)..... 21

18 U.S.C. § 2520..... 21

18 U.S.C. § 2707..... 21

18 U.S.C. § 2712..... 2, 20, 21, 23

1 18 U.S.C. § 2712(a) 21
 2 18 U.S.C. § 2712(b)(3) 22
 3 18 U.S.C. § 2712(b)(4) 2, 17, 18, 19, 20, 21, 22
 4 50 U.S.C. § 1806(f) 2, 17, 18, 19, 21, 22

5

6 **Rules**

7 Fed. R. Civ. Pro. 56(c)(2) 3
 8 Fed. R. Evid. 701 11
 9 Fed. R. Evid. 801(d)(2)(D) 9, 12
 10 Fed. R. Evid. 803(3) 10, 12
 11 Fed. R. Evid. 803(6) 9
 12 Fed. R. Evid. 901(a) 5
 13 Fed. R. Evid. 901(b)(4)..... 5

14

15 **Other Authorities**

16 George Molczan, *A Legal And Law Enforcement Guide To Telephony* (2005)..... 6

17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

1 **INTRODUCTION**

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

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

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

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

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

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

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

- 4 • Plaintiffs’ public evidence also establishes that at least one of their Internet metadata
5 records was included in what the Foreign Intelligence Surveillance Court described
6 as the “massive” and “wholly non-targeted bulk production” of Internet metadata.

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

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

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

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

- 27 • Plaintiffs are aggrieved persons under the standard adopted by this Court in the
28 related *In re NSA* multidistrict litigation because their “allegations ‘are sufficiently

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

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

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

17 ARGUMENT

18 **I. Plaintiffs Have Proffered Sufficient Public Evidence Of Their Standing To Defeat** 19 **Summary Judgment And To Proceed To The Merits Using Classified Evidence**

20 The government’s attack on the sufficiency of plaintiffs’ evidence makes three critical
 21 errors.

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

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

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

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

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

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

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

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

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

6 The government's authenticity challenge is meritless. Authentication "does not erect a
7 particularly high hurdle." *U.S. v. Dhinsa*, 243 F.3d 635, 658 (2d Cir. 2001). "The appearance,
8 contents, substance, internal patterns, or other distinctive characteristics of the item, taken together
9 with all the circumstances" can be "sufficient to support a finding that the item is what the
10 proponent claims it is." Fed. R. Evid. 901(a), (b)(4). The appearance, contents, substance, internal
11 patterns, and other distinctive characteristics of the NSA Letter and the NSA Inspector General's
12 Report of which it is a part, taken together with the circumstances of its production by the
13 government in FOIA litigation seeking only NSA Inspector General Reports, is sufficient to
14 authenticate the NSA Letter. Indeed, the government's production of the NSA Letter is by itself a
15 judicial admission of its authenticity. *Orr v. Bank of America*, 285 F.3d 764, 777 n.20 (9th Cir.
16 2002). And, if more is needed, counsel for the New York Times in its FOIA litigation against the
17 NSA confirms that the NSA Letter was produced by the NSA. McCraw Decl. ¶¶ 5-6.

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

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

24 Plaintiffs' additional evidence also supports their standing. Plaintiffs were AT&T and
25 Verizon customers. The government objects to the conclusion—a deduction based on evidence,
26 not speculation—that a phone records program that excluded both AT&T (with 163 million
27
28

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

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

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

19 _____
 20 ¹ AT&T Inc.’s SEC Form 8-K, at 2-3 (July 24, 2018), available at
 21 <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.

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

24 ³ The government makes a silly objection to plaintiffs’ citation to a learned treatise for the fact that
 25 a phone call between customers of two different phone companies generates two phone records—
 26 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
 27 reasonable dispute—and not disputed by the government—and easily “‘could be presented in an
 28 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).

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

12 **B. Plaintiffs Have Standing To Challenge The Government’s Interference With**
13 **Their Internet Communications**

14 **1. Plaintiffs’ Evidence Of The Government’s Interference With Their**
15 **Internet Communications Is Competent And Admissible**

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

21 **(a) The AT&T Documents Attached To The Klein Declaration**
22 **Are Authentic**

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

26 [REDACTED]

27 [REDACTED]

28 [REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[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]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]

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

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

27 Second, the AT&T documents are admissible as AT&T business records. Fed. R. Evid.
28 803(6). Rule 803(6) includes not only records of “acts” but also “events” and “conditions” (two

1 categories omitted by the government, Govt. Reply at 16); this language easily encompasses
2 AT&T's implementation and operation of a surveillance facility on behalf of the government. And
3 despite the government's unsupported protestations, operating surveillance devices on behalf of the
4 government is a regularly conducted activity of AT&T, as AT&T's transparency reports
5 demonstrate. ECF No. 417-4, Ex. C. Because these surveillance devices are integrated into it
6 AT&T's Internet backbone, they are integrated into its other regularly conducted activities; it is
7 crucially important that they operate in harmony with the rest of AT&T's network and not disrupt
8 Internet transmissions. Marcus Decl. ¶¶ 34, 60, 62, 116; ECF No. 417-6 (Reid Decl.), ¶¶ 22, 53-
9 57, 63-64; ECF No. 417-7 (Blaze Decl.), ¶¶ 38, 56.

10 Finally, the government contends the documents are inadmissible hearsay because they are
11 only a statement of plan or intent. This ignores Russell's independent testimony and the hearsay
12 exceptions for business records and statements of an agent. Even apart from those, the government
13 is wrong because statements of plan or intent are admissible to show the declarant thereafter acted
14 in accordance with the stated intent. Fed. R. Evid. 803(3) (statements reflecting plan or intent are
15 admissible); *U.S. v. Best*, 219 F.3d 192, 198 (2d Cir. 2000) (statement of plan or intent can be used
16 to "prove that the declarant thereafter acted in accordance with the stated intent"); *U.S. v. Donley*,
17 878 F.2d 735, 737-38 (3d Cir. 1989) (same); *U.S. v. Astorga-Torres*, 682 F.2d 1331, 1335 (9th Cir.
18 1982) (same). So even if the AT&T documents were only future plans for surveillance devices,
19 they are admissible to show AT&T thereafter installed and operated those devices as the
20 documents reflect.

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

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

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

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

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

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

20
21 ⁴ *Accord U.S. v. Famaia-Roche*, 537 F.3d 71, 76 (1st Cir. 2008) (low-level drug dealer could
22 testify to activities and drug sales by other drug dealers in narcotics organization she was part of);
23 *DIRECTV, Inc. v. Budden*, 420 F.3d 521, 529 (5th Cir. 2005) (employee could testify about facts
24 concerning another company he learned through a law enforcement investigation); *U.S. v. Doe*, 960
25 F.2d 221, 223 (1st Cir. 1992) (gun shop owner could testify that pistol sold to him by another
26 United States company was manufactured in Brazil); *White v. MPW Indus. Servs., Inc.*, 236 F.R.D.
27 363, 369 (E.D. Tenn. 2006) (“employees . . . would have learned during the normal course of their
28 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).

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

3 Thus, Klein is competent to testify about his personal knowledge and observations on the
4 job regarding AT&T's relationship with the NSA. This evidence includes the following: Klein,
5 who otherwise had keys and free access to all parts of AT&T's Folsom Street Facility, has personal
6 knowledge that the reason he was excluded only from the AT&T secure room is because AT&T's
7 policy was to restrict access to only persons cleared by the NSA, even in emergencies. Klein Decl.
8 ¶¶ 17, 18. AT&T employee Philip Long confirms that AT&T restricted access to the secure room.
9 ECF No. 417-5 (Long Decl.), ¶ 21. Likewise, Klein testified from his personal knowledge about
10 visiting the AT&T secure room while it was under construction (where he saw AT&T employee
11 "FSS #2," whom Klein had observed meeting with an NSA agent and whom Klein knew to be in
12 charge of the room, installing equipment) and of again entering the AT&T secure room after it was
13 in operation. *Id.* at ¶¶ 10, 12, 14, 17. And Klein's statements that "The NSA agent came and met
14 with FSS #2" and "The NSA agent did come and speak to [AT&T employee] FSS #1" are also
15 direct personal observations, not hearsay. *Id.* at ¶¶ 10, 16.

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

26 The e-mail to Klein from AT&T management regarding the NSA and the statements to
27 Klein by his manager and a co-worker telling of upcoming visits by an NSA agent (Klein Decl.
28 ¶¶ 10, 14, 16) are independently admissible under Federal Rule of Evidence 803(3) as statements

1 of future intention to meet with the NSA, that the intended purpose of the first meeting was that
 2 “the NSA agent was to interview FSS #2 for a special job” managing the AT&T secure room, that
 3 the intended purpose of the second meeting was to discuss “FSS #3’s suitability to perform the
 4 special job that FSS #2 had been doing,” and that AT&T’s management’s plan and intent was to
 5 cooperate with the NSA. Further, they are also evidence that AT&T employees actually met with
 6 NSA agents and managed the AT&T secure room to facilitate the NSA’s purposes, and that AT&T
 7 did cooperate with the NSA. *Best*, 219 F.3d at 198 (statement of plan or intent can be used to
 8 “prove that the declarant thereafter acted in accordance with the stated intent”); *Donley*, 878 F.2d at
 9 737-38; *Astorga-Torres*, 682 F.2d at 1335.

10 **2. Who Holds The Keys To The AT&T Secure Room Is Irrelevant To** 11 **Plaintiffs’ Standing**

12 The government erroneously contends that it is essential to plaintiffs’ standing that they
 13 show that the NSA controls the operation of the AT&T secure room. Govt. Reply at 16.

14 Apparently, the government is relying on some secret argument that it is not liable because AT&T
 15 operates the equipment that performs the surveillance the NSA orders.

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

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

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

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

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

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

21 Given the government’s focus on “copying” and its suggestion that plaintiffs are mistaken
22 about whether or how their communications are copied (Govt. Reply at 12, 17), plaintiffs surmise
23 that the government has a secret theory of nonliability that it has deployed in its classified
24 submissions. It may be that the government contends that no copying occurs at all, but if so that
25 would just be a factual dispute precluding summary judgment. As plaintiffs’ experts have
26 explained, intercepting, filtering, and selecting communications from the Internet backbone based
27 on their email addresses requires some form of copying and reassembly of the email message.
28 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

1 way’”).

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

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

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

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

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

24 The NSA Draft OIG Report is yet further evidence showing AT&T’s and Verizon’s
25 participation in Internet backbone surveillance. ECF No. 417 at 9 n.6, 15; ECF No. 147, Ex. A at
26 27-29, 33-34. It also evidences AT&T’s and Verizon’s participation in the phone records program
27 and the Internet metadata program. ECF No. 417 at 9 & n.6, 19-20. The government disputes the
28 authenticity of the NSA Draft OIG Report. It is undisputed that the NSA Inspector General

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

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

16 **C. Plaintiffs Have Standing To Challenge The Government's Collection Of**
17 **Internet Metadata**

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

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

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

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

8 Indeed, the indeterminate, ever-changing, and essentially random nature of Internet
9 communications routing means that wherever on the Internet backbone the Internet metadata
10 collection devices may have been located, over the years it is more probable than not that at least
11 one of each plaintiffs' communications passed through it. Reid Decl. ¶¶ 21, 23, 26-30, 34-36, 48-
12 57, 62-64; Blaze Decl. ¶¶ 15, 21, 26, 40, 42-43.

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

15 Finally, it is possible that the surveillance devices at AT&T's Folsom Street facility, and
16 whatever other devices the NSA has used for Internet backbone surveillance, were also used to
17 collect Internet metadata. As plaintiffs' experts explain, in order to collect the "to" and "from"
18 email addresses that the government characterizes as "metadata," it is necessary to reconstruct and
19 examine the content of the email message. Reid Decl. ¶¶ 22(c), 59-61; Blaze Decl. ¶¶ 12, 22, 27,
20 33, 38. So any Internet metadata collection program is necessarily copying, at least temporarily,
21 and examining the content of the emails whose metadata it is collecting. If the Internet backbone
22 surveillance devices at AT&T's Folsom Street facility and elsewhere were used to collect Internet
23 metadata as well, then the same evidence that shows plaintiffs' standing to challenge Internet
24 content surveillance also gives them standing to challenge Internet metadata collection.

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

28 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

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

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

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

14 **A. The Court Must Use The Classified Evidence In Deciding The Merits**

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

17 In granting partial summary judgment to plaintiffs in 2013, the Court squarely, and
18 correctly, held that Congress preempted the state secrets privilege with section 1806(f) and section
19 2712(b)(4).⁵ *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1097, 1103, 1104-05, 1112 (N.D. Cal. 2013).
20 Since then, the Court has twice reiterated that holding. ECF Nos. 347 at 1-2; 340 at 2.

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

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

26 _____
27 ⁵ The government makes the odd and unsupported argument that plaintiffs have abandoned section
28 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.

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

4 The government argues that section 1806(f) and section 2712(b)(4) do not preempt the state
5 secrets privilege, but it presents no grounds justifying reconsideration by the Court of its 2013
6 ruling that those statutes preempt the privilege. Govt. Opening Br. at 23; Govt. Reply at 27.
7 Instead, it ignores the Court’s ruling and pretends that the Court has never ruled on the preemption
8 issue. (Previously, the government freely admitted that “[t]he Court . . . held that section 1806(f)
9 preempts application of the state secrets privilege in these cases.” ECF No. 167 at 4; *see id.* at
10 6-7.) The government likewise ignores the Ninth Circuit’s conclusion in *Mohamed* that when
11 Congress enacts statutory schemes like section 1806(f), it preempts the state secrets privilege.

12 But this Court’s rulings, and those of the Ninth Circuit, may not be evaded simply by
13 ignoring them. Those rulings remain correct for all of the reasons previously stated by the Court
14 and all of the reasons plaintiffs have presented. *See Jewel*, 965 F. Supp. 2d at 1097, 1103-05,
15 1112; ECF Nos. 417 at 28-29; 407 at 4-5; 140 at 4-7; 112 at 2-13; 83 at 12-22.

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

17 As plaintiffs’ opening brief explains, plaintiffs meet any standard for using section
18 2712(b)(4) or section 1806(f), including the “aggrieved person” standard. ECF 417 at 23-28.

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

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

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

1 Plaintiffs are aggrieved persons under the “zone of interests” test because they come within
2 the zone of interests of the Wiretap Act, the SCA, and section 2712. *Dir., Office of Workers’*
3 *Comp. Prog. v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 127 (1995); *Jewel*,
4 673 F.3d at 913.

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

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

9 This argument is foreclosed by the Court’s prior rulings. The Court has ruled that, as the
10 plain language of the statute provides, section 2712(b)(4) displaces the state secrets privilege and
11 governs the use of classified evidence for claims brought under section 2712. *Jewel*, 965 F. Supp.
12 2d at 1104-05, 1112; ECF No. 347 at 1-2; ECF No. 340 at 2.

13 The Court has also rejected the government’s argument that section 2712 is limited to
14 malicious-leak claims. The Court held that section 2712’s cause of action encompasses plaintiffs’
15 claims because it applies to any violation of the Wiretap Act or the SCA, not just claims for the
16 unlawful use or disclosure of communications or communications records: “The plain language of
17 Section 2712(a) does not limit the waiver of sovereign immunity for damage claims under the SCA
18 and the Wiretap Act to claims for the use and disclosure of information.” *Jewel*, 965 F. Supp. 2d at
19 1107. The Ninth Circuit also held that plaintiffs’ statutory claims are proper. *Jewel*, 673 F.3d at
20 913.

21 Even if the issue of section 2712’s scope were not foreclosed, the government’s argument
22 would lack merit. The government relies on a snippet from a single senator to argue that section
23 2712 is limited to claims of malicious leaks. Govt. Reply at 28. The government badly misstated
24 the legislative history of section 2712 in the proceedings leading up to the Court’s 2013 order.
25 ECF No. 140 at 6-7 & n.3 (explaining section 2712’s legislative history); ECF No. 133 (12/14/12
26 RT) at 106-107. The government again gets it wrong. While section 2712 certainly encompasses
27 malicious leaks, nothing in the senator’s statement suggests the statute is limited to leaks. The
28 statement focuses on liability for leaks because that liability was newly created in section 2712,

1 while liability for Wiretap Act and SCA violations had existed previously in 18 U.S.C. § 2520 and
2 18 U.S.C. § 2707 and was merely being transferred to section 2712 by the USA PATRIOT Act.

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

13 Finally, the government argues that plaintiffs can never be aggrieved persons under section
14 2712 because 18 U.S.C. § 2510(11) links *its* definition of “aggrieved person” to the interception of
15 communications. Govt. Reply at 29-31. But the government ignores that section 2712, including
16 section 2712(b)(4) and its incorporation of section 1806(f)’s procedures, applies to “[a]ny person
17 who is aggrieved by any willful violation of this chapter [the SCA] or of chapter 119 [the Wiretap
18 Act]”—a provision that extends beyond communications interceptions under the Wiretap Act to
19 encompass communications records violations under the SCA. 18 U.S.C. § 2712(a). Plaintiffs’
20 claims thus are within the scope of sections 2712(a) and 2712(b)(4), as the Court has held.

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

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

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

4 As plaintiffs' opening brief explains, section 2712(b)(4) extends the scope of section
5 1806(f) to encompass not only merits determinations but any other determination, including
6 standing. ECF 417 at 23-24. And as explained in plaintiffs' opening brief and above, plaintiffs
7 have met any test for using sections 2712(b)(4) and 1806(f), including showing they are aggrieved
8 persons. ECF 417 at 24-28.

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

9
10 The government contends that litigating standing would result in the disclosure of
11 additional reams of secret evidence. Govt. Reply at 19-22. This argument lacks merit.

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

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

26 If instead it finds that plaintiffs have standing, it need not issue any opinion at all at that
27 time, but can proceed to the post-standing merits phase.
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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