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)
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,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

CASE NO. 08-CV-4373-JSW

PLAINTIFFS' OPPOSITION TO THE GOVERNMENT'S SUMMARY JUDGMENT MOTION AND PLAINTIFFS' MOTION TO PROCEED TO RESOLUTION ON THE MERITS USING THE PROCEDURES OF SECTION 1806(f)

Courtroom 5, Second Floor
The Honorable Jeffrey S. White

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Directives

Other Authorities

NOTICE OF MOTION AND MOTION

PLEASE TAKE NOTICE that on a date and time to be determined by the above-entitled Court, located at the United States District Court, 1301 Clay Street, Oakland, California, plaintiffs will move the Court, pursuant to the Court's order dated August 17, 2018, for an order:

1. Denying the motion for summary judgment on plaintiffs' standing for their statutory claims under section 2712 of title 18 U.S.C. for violations of the Wiretap Act (18 U.S.C. §§ 2510 et seq.), and the Stored Communications Act (18 U.S.C. §§ 2701 et seq.), brought by government defendants United States, National Security Agency, Department of Justice, and official-capacity defendants Paul Nakasone, Donald Trump, Jefferson Sessions, and Daniel Coats; and

2. Ordering that the case proceed to discovery on the merits and resolution on the merits, using public evidence and classified evidence reviewed *ex parte* and *in camera* to decide all remaining issues, including whether the surveillance was "lawfully authorized and conducted." *See* 18 U.S.C § 2712(b)(4); 50 U.S.C. § 1806(f).

This opposition and motion is based on this notice of motion and motion, the proposed order filed herewith, the Declaration of Richard R. Wiebe in Support of Plaintiffs' FRCP 56(d) Request for Further Discovery on Standing, Declaration of Cindy A. Cohn in Opposition to the Government's Motion for Summary Judgment, Declaration of David A. Greene in Opposition to the Government's Motion for Summary Judgment, Declaration of Richard R. Wiebe in Opposition to the Government's Motion for Summary Judgment, Declaration of Phillip Long, Declaration of Dr. Brian Reid, Declaration of Professor Matthew Blaze, Declaration of Ashkan Soltani, Declaration of Carolyn Jewel in Opposition to the Government Defendants' Motion for Summary Judgment, Declaration of Tash Hepting in Opposition to the Government Defendants' Motion for Summary Judgment, Declaration of Young Boon Hicks in Opposition to the Government Defendants' Motion for Summary Judgment, Declaration of Erik Knutzen in Opposition to the Government Defendants' Motion for Summary Judgment, the Declaration of Joice Walton in Opposition to the Government Defendants' Motion for Summary Judgment, and the sealed declarations of Mark Klein (ECF No. 84-4), Scott Marcus (ECF No. 89) and James Russell (ECF No. 84-1), all previously filed in this litigation.

MEMORANDUM

Introduction

Just this past term, Chief Justice Roberts explained in the landmark case *Carpenter v. United States* that "seismic shifts in digital technology [have] made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."

Carpenter arose from government access to only one of the pieces of information about Americans available through the "ever alert" and "infallible memories" of service providers like AT&T: cellphone location records. This case involves far deeper intrusions into personal privacy. Plaintiffs here seek to protect the privacy of their communications with friends, colleagues, clergy, medical professionals and loved ones, their political and other associations, search queries, reading history, social media postings, and more.

Congress passed the Wiretap Act and the Stored Communications Act to protect ordinary Americans like plaintiffs, not suspected of any crime, against governmental surveillance. In enacting 18 U.S.C. § 2712 as part of the USA PATRIOT Act in 2001, Congress made sure that those statutes reach national security surveillance as well as domestic surveillance. Congress expressly cleared a procedural pathway for a judicial determination of legality, even when secret evidence is relevant. In the Ninth Circuit's words, "[I]n the surveillance statutes, by granting a judicial avenue of relief, Congress specifically envisioned plaintiffs challenging government surveillance under this statutory constellation." *Jewel v. NSA*, 673 F.3d, 902, 913 (9th Cir. 2011).

This case asks whether these statutes, along with the Constitution, allow the government, in the words of the Supreme Court in *Carpenter*, to turn those "ever alert" service providers into a tool of mass surveillance of "everyone else." After 12 years of litigation arising from these mass surveillance programs, ten in this current case, plaintiffs, and all Americans, deserve an answer to that question.

But instead, plaintiffs are being required to relitigate two issues well-known to this Court.

Plaintiffs must, once again, address the arguments that, notwithstanding Congress' clear directive in 18 U.S.C. § 2712 to use classified evidence to resolve issues on their merits, the state secrets privilege requires dismissal of this case—arguments that the government first raised in 2006 and that this Court rejected five years ago.

And Plaintiffs are being required, once again, demonstrate their standing.

Standing is established once this Court finds that it is *more likely than not* that the government's admitted mass surveillance over the past 17 years touched, even for an instant, a single email, website visit, search, or Internet communication of each of the five plaintiffs, and that their phone records and Internet metadata were included in the government's mass, indiscriminate collection. Whether even momentary touching amounts to a statutory violation, as well as whether factually, all that occurred here was momentary touching, are disputed questions for the merits, not standing.

The evidence here is more than sufficient to reach the conclusion that plaintiffs have standing. The direct evidence includes the authenticated AT&T documents, which describe a system that touches a tremendous amount of domestic Internet traffic, specifically including AT&T's Folsom Street facility in San Francisco. A new witness, Philip Long, here confirms that he was ordered to divert a large amount of domestic Internet traffic to this facility without any technological or business justification. Longstanding witness Mark Klein, plus the AT&T documents, show that when traffic arrived at Folsom Street for peering, a copy was made for submission to the surveillance infrastructure. Three new experts, Matt Blaze, Brien Reid and Ashkan Soltani, along with original expert J. Scott Marcus, confirm that the admitted infrastructure, along with basic Internet processes, make it more likely than not that at least one of each plaintiff's communications was diverted.

The government's public admissions leave no doubt that the surveillance systems described by the witnesses and AT&T documents touched trillions of communications and communications records of tens of millions of nonsuspect Americans. In government reports and publicly released decisions of the Foreign Intelligence Surveillance Court (FISC), the programs have been described as "massive" and involving "the collection of both a huge volume and a high percentage of

unrelated communications" (Internet metadata); involving phone records searches that examined the records of over 120 million persons in a single year (telephone records); and interceptions "in the flow of communications between communication service providers" (Internet backbone surveillance).

These facts easily meet the "more likely than not" standard. And there can be no serious claim that it would harm national security if the Court finds that plaintiffs—ordinary nonsuspect customers of telecom giant AT&T—were five of the hundreds of millions of Americans touched by these massive surveillance programs over the past 17 years.

The government's opposing argument strains both the law and credulity. Ignoring the more-likely-than-not standard, the government wrongly claims that the standing doctrine requires this court to accept the remote theoretical possibility that the programs may have magically excluded every single communication or communications record of the plaintiff. The government's argument at bottom is that, although it has admittedly touched at least tens of millions of nonsuspect Americans and billions of their communications, as long as it does not admit to touching any particular one of those communications, none of those Americans has standing to challenge the sweep of the programs. That is not the law. This attempt to convince the court to adopt a misstatement of law is the government's latest attempt to avoid the fact that the evidence – much of it admitted by the government in response to public concern about these programs impacting nonsuspect Americans -- shows a likelihood that the plaintiffs suffered an injury-in-fact.

Finally, standing is not a game of three-card monte. The secret evidence submitted by government should demonstrate conclusively that plaintiffs were touched by the admitted mass surveillance, and it should be used. Plaintiffs should be allowed to go forward under the statutory mandate of 18 U.S.C. § 2712 and 50 U.S.C. § 1806(f), which require a judicial determination, after review of the classified information provided by the government, of the issues presented in this litigation, including standing and whether the surveillance was lawfully authorized and conducted.

Argument

I. The Government Cannot Meet Its Summary Judgment Burden.

A. Plaintiffs' Burden In Opposing Summary Judgment On Standing

Plaintiffs' burden in opposing summary judgment on the issue of standing is only to produce sufficient evidence from which a reasonable factfinder could conclude it is more likely than not that the government has interfered with their communications and communications records, thereby creating a triable issue of fact. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986); *Fresno Motors, LLC v. Mercedes Benz USA, LLC*, 771 F.3d 1119, 1125 (9th Cir. 2014). If plaintiffs meet that burden, they are entitled to proceed to discovery on the merits and, ultimately, trial.

In deciding whether plaintiffs' evidence is sufficient, the court must view the evidence in the light most favorable to plaintiffs and draw all inferences in plaintiffs' favor. *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011); *ACLU of Nevada v. Las Vegas*, 466 F.3d 784, 790-91 (9th Cir. 2006). Drawing inferences regarding standing in plaintiffs' favor is especially critical here, where plaintiffs have been denied many of the basic rights granted to all other litigants. Plaintiffs have been denied access to *any* of the defendants' discovery responses revealing new information. They have been deprived of the right to have the government answer requests for admission with an admission or denial, as the Federal Rules require. Finally, Plaintiffs and the Court have been permanently denied many years' worth of information directly relevant to the issue of standing due to the government's spoliation of the evidence.[1]

Thus, the Court may grant summary judgment to the government only if, viewing all the evidence and inferences in the light most favorable to plaintiffs, *no* reasonable factfinder could conclude it was likely that over the many years of the government's surveillance at least one of each plaintiff's communications was copied or redirected or that at least one of their phone records or Internet metadata records was collected.

[1] Plaintiffs have filed a declaration under Fed. R. Civ. Pro. 56(d) explaining why the denial of their discovery rights precludes any grant of summary judgment to the government. Wiebe Rule 56(d) Decl.

B. Disputed And Intertwined Questions Of Standing And the Merits Cannot Be Resolved at the Standing Stage On Summary Judgment

If "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). This rule applies here because the facts showing the government's copying of plaintiffs' communications and collection of their communications records are material to both standing and the merits. Thus, if the Court concludes there is a genuine dispute as to those facts, it may not decide standing in summary proceedings.

C. The Ninth Circuit's Previous Rulings Frame the Question of Standing.

In the prior appeal, the Ninth Circuit laid to rest several basic questions about plaintiffs' standing. First, "three requirements . . . must be met for Article III standing: (1) an injury-in-fact that (2) is fairly traceable to the challenged conduct and (3) has some likelihood of redressability." *Jewel*, 673 F.3d at 908. The Ninth Circuit held that only injury-in-fact is at issue here, and that traceability and redressability are satisfied.[2]

Second, it is law of the case that standing does not require plaintiffs to show that they are aggrieved persons. *Jewel*, 673 F.3d at 907 n.4 (whether plaintiffs are "'Aggrieved Person[s]'" "is a merits determination, not a threshold standing question.").

Third, to show injury-in-fact plaintiffs need not show that the Wiretap Act or the Stored Communications Act (SCA) have been violated. *Jewel*, 673 F.3d at 907 n.4 ("[W]hether a plaintiff states a claim for relief typically relates to the merits of a case, not to the dispute's justiciability."). Indeed, in the prior appeal, the Ninth Circuit warned this Court against "conflat[ing] the ultimate merits question—whether the surveillance exceeded statutory or constitutional authority—with the threshold standing determination." *Id*. at 911 n.5. Standing "in no way depends on the merits of

[2] The Ninth Circuit held there is no dispute that the mass interceptions of Internet communications content and the bulk collection of phone records and Internet metadata are traceable to the government defendants' surveillance programs (the second element). *Jewel*, 673 F.3d at 912 ("[T]he harms Jewel alleges—invasion of privacy and violation of statutory protections—can be directly linked to this acknowledged surveillance program."). There is also no doubt that section 2712 provides an avenue of redress for plaintiffs' claims (the third element). *Id.* ("There is no real question about redressability.")

the plaintiff's contention that particular conduct is illegal." *Warth v. Seldin*, 422 U.S. 490, 500 (1975).

Within this framework, plaintiffs 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 v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). In doing so, plaintiffs may use any combination of direct and circumstantial evidence that taken together shows injury-in-fact.

D. Injury-in-fact Occurs When The Government's Mass Surveillance Systems Touch A Single Communication Or Communication Record of Plaintiffs

Injury-in-fact asks whether plaintiffs have suffered injury to a legally protected interest. Injury-in-fact is "an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560. Quantitatively, the "invasion" of the interest need not be substantial: "'an identifiable trifle is enough for standing.'" *U.S. v. SCRAP*, 412 U.S. 669, 689 n.14 (1973) (citing numerous examples), *quoted in Council of Ins. Agents & Brokers v. Molasky-Arman*, 522 F.3d 925, 932 (9th Cir. 2008).

It is law of the case that plaintiffs have legally protected privacy interests in their Internet communications and in their telephone and Internet communications records. *Jewel*, 673 F.3d at 908, 913. Indeed, as noted above, the privacy interests plaintiffs assert stand at the heart of the Wiretap Act and the SCA: "Congress specifically envisioned plaintiffs challenging government surveillance under this statutory constellation." *Id*. at 913. That statutory constellation includes 18 U.S.C. section 2712(b)(4), which gives the courts the classified evidence necessary to decide all the issues—including standing—and the duty to use that evidence.

As stated, the quantum of interference with plaintiffs' communications and communications records required to establish an injury sufficient for their standing on each claim—"an identifiable trifle"—is minimal:

For their Wiretap Act claim, injury-in-fact occurred for each plaintiff when any *one* of their communications traveling on the Internet backbone was intercepted, copied, or redirected (for example, by a splitter or other similar technologies) diverting it from its normal course of

transmission.[3] That is far more than an "identifiable trifle." It is an injury-in-fact, and is so regardless of what happens to plaintiffs' communications after they have been redirected, even if those communications are never permanently stored and even if they are immediately discarded. To defeat summary judgment, plaintiffs need only show that a reasonable factfinder could conclude it is more likely than not that this copying and redirection occurred with one of their Internet communications.

For their SCA phone records claim, the bulk collection of phone records from plaintiffs' telephone companies is an injury-in-fact sufficient to establish plaintiffs' standing. As the Second Circuit confirmed, ordinary phone customers whose records were collected as part of this program "surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them." *ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015). To defeat summary judgment, each of the plaintiffs need only show a reasonable factfinder could conclude it is more likely than not that at least one of their phone records was collected. [4]

For their Internet metadata claim, the bulk collection of Internet metadata from Internet service providers similarly is an injury-in-fact sufficient to establish plaintiffs' standing. To defeat summary judgment, plaintiffs need only show a reasonable factfinder could conclude it is more likely than not that at least one of their Internet metadata records was collected.

II. The Public Evidence Demonstrates Plaintiffs' Standing

A. Phone Records

The public evidence demonstrates that it is more likely than not that at least one phone record of each plaintiff was obtained by the government as part of its bulk collection of phone

[3] "[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time." *George v. Carusone*, 849 F. Supp. 159, 163 (D.Conn. 1994) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992), *cert. denied,* 506 U.S. 847 (1992)).

[4] *See e.g. Konop v. Hawaiian Airlines*, Inc., 302 F.3d 868, 878 (9th Cir. 2002). (for website, construing "intercept" in light of ordinary meaning, i.e., "to stop, seize, or interrupt in progress or course before arrival.") (citation omitted); *see also U.S. v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005) (en banc) (acquisition of emails from electronic storage intrinsic to the transmission process constitutes interception).

records starting in 2001, which is all that plaintiffs need show to establish an injury-in-fact.

The Foreign Intelligence Surveillance Court (FISC) has described the phone records program as "the ongoing production by major telephone service providers of call detail records for all domestic, United States-to-foreign, and foreign-to-United States calls." Greene Decl., Ex. A (FISC "PR/TT Order") at 74. The Privacy and Civil Liberties Oversight Board (PCLOB) confirms that "millions of telephone numbers [were] covered by the NSA's Section 215 program," and that for each, "the agency obtains a record of all incoming and outgoing calls." Cohn Decl., Ex. A ("PCLOB 215 Report") at 115.

"[T]he companies are directed to supply virtually all of their calling records to the NSA . . . the NSA has described its program as enabling 'comprehensive' analysis of telephone communications 'that cross different providers and telecommunications networks.' The vast majority of the records obtained are for purely domestic calls, meaning those calls in which both participants are located within the United States, including local calls." *Id*. at 22.

That mass collection included plaintiffs. Since 2001, when the government began collecting phone records in bulk, all plaintiffs have been phone customers of AT&T, plaintiffs Hepting and Walton have been Verizon customers, and certain plaintiffs have been customers of T-Mobile, Qwest, Cingular, and/or Virgin Mobile, as well. PCLOB 215 Report at 37; Declaration of Carolyn Jewel ("Jewel Decl.") ¶¶ 22-23; Declaration of Tash Hepting ("Hepting Decl.") ¶¶ 18-20; Declaration of Young Boon Hicks ("Hicks Decl.") ¶¶ 4-5; Declaration of Erik Knutzen ("Knutzen Decl.") ¶¶ 20-22; Declaration of Joice Walton ("Walton Decl.") ¶¶ 20-24.

The government has admitted in declassified FISC documents that AT&T, Verizon, Verizon Wireless, and Sprint were part of the phone records program and produced phone records in bulk. Wiebe Decl. ¶¶ 3, 4 and Exs. A, B.[5] The government has also released a FISC order

[5]Exhibit A is a primary order for bulk production of phone records from multiple phone companies issued in FISC docket BR 10-10 ("BR" for "Business Records"). Exhibit B is an excerpt from an NSA compliance audit that includes a letter from the NSA to the FISC reporting a non-compliance incident. The caption to the letter identifies the phone companies that were compelled by primary order BR 10-10 to produce their phone records in bulk as AT&T, Verizon, Verizon Wireless, and Sprint. Ex. B, pp. 28-29. The PCLOB 215 Report at p. 54 discusses the non-compliance incident (incident "(2)") that is the subject of Exhibit B, further corroborating Exhibit B's authenticity.

admitting the participation of Verizon Business Network Services (formerly MCI/Worldcom) in the phone records program. ECF No. 144, Ex. A at 1, 4; ECF No. 178, Ex. D at 4.

Additional evidence corroborates the admitted participation of AT&T and Verizon. The NSA Draft OIG Report confirms AT&T and Verizon were part of the phone records program.[6]

In addition to these factual admissions, the government's admitted purpose for the phone records program confirms that it could not have operated without the participation of AT&T, the largest phone company. The purpose of the phone records program was to assemble a set of phone records so comprehensive that three-hop contact chaining could be conducted. Three-hop contact chaining means selecting a target person, looking at the target's phone records to see everyone the target called (first hop), looking at the phone records of everyone the target called to see who they called (second hop), and looking at the phone records of everyone called by someone who was called by the target to see who *they* called (third hop). PCLOB 215 Report at 29-31, 115, 143. The third hop can result in looking at the phone records of hundreds of thousands of persons. *Id*. at 29. The PCLOB estimated that the three-hop searches conducted by the NSA in 2012 alone yielded the phone records of 120 million persons. *Id*. at 30-31. And these are the search *results*, the initial collection is necessarily much larger—almost 2 billion records a day from one provider in 2011. Wiebe Decl., Ex. E. Three-hop contact chaining required the government to collect the phone records of hundreds of millions of persons on an ongoing basis.

To deny the existence of standing, the Court would have to hold that it is not likely that AT&T participated in the telephone records program. That would be absurd, and not just because the government has admitted AT&T's participation. Excluding AT&T, the largest United States phone company, would have rendered the phone records program ineffectual at performing the

---

[6] ECF No. 147, Ex. A at 33-34. The NSA Draft OIG Report describes the NSA's relationship with "Company A" and "Company B." *See id*. at 27-29, 33-34. From the PSP's inception, Companies A and B participated in the interception of Internet content and provided Internet metadata and telephone call records. *Id*. at 33-34. The NSA's relationship with them are among its "most productive," providing access to large volumes of communications "transiting the United States through fiber-optic cables, gateway switches, and data networks." *Id*. at 28-29. Company A and Company B were the two largest providers of international telephone calls into and out of the United States. *Id.* at 27. AT&T and MCI/Worldcom (which later merged with Verizon) were the country's two largest international telephone call providers at that time. ECF No. 262, Ex. E.

central task of contact chaining.[7] Once the government's non-AT&T phone records led to an AT&T number, contact chaining would have hit a wall. *See ACLU v. Clapper*, 785 F.3d at 797 ("The government . . . does not seriously dispute appellants' contention that all significant service providers in the United States are subject to similar orders."). "'As FISC Judge Eagan noted, the collection of virtually all telephony metadata is "necessary" to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine "connections between known and unknown international terrorist operatives."'" *Jewel v. NSA*, 2015 WL 545925, *3 (N.D. Cal. Feb. 10, 2015), quoting *ACLU v. Clapper*, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013).

To deny standing, the Court would also have to find that Verizon, the second-largest carrier, did not likely participate, despite the government's admissions that it did. Moreover, Verizon's phone records also include records of all the calls of *non*-Verizon phone customers that are calls to or from any of Verizon's many millions of customers. George Molczan, *A Legal And Law Enforcement Guide To Telephony*, pp. 34, 38 (2005) (Wiebe Decl., Ex. F). So even if only Verizon had participated in the phone records program—which is inconceivable—it is a practical certainty that the billions of Verizon records acquired over 14 years by the government would contain records of calls to or from the non-Verizon plaintiffs, as well as the Verizon plaintiffs.

Drawing all inferences in plaintiffs' favor, a rational factfinder could conclude that it is more probable than not that at least one of each plaintiffs' phone records has been collected.

B. Internet Interception

1. Plaintiffs have standing for their Wiretap Act Internet interception claims from the Internet backbone.

The evidence demonstrates that it is more likely than not that since 2001 *at least one* Internet communication of each plaintiff was initially copied and redirected as it transited the Internet backbone. That is all that plaintiffs need show to establish an injury-in-fact for their Wiretap Act Internet interception claims.

[7] Antoine Gara, "The World's Largest Telecom Companies: AT&T And Verizon Top China Mobile," Forbes, (May 24, 2017), *available at* https://www.forbes.com/sites/antoinegara/2017/05/24/the-worlds-largest-telecom-companies-att-and-verizon-top-china-mobile/#16998737a452.

The government admits the following:

NSA's Internet backbone surveillance started in 2001 under the PSP and continued after 2006 under FISC orders. Cohn Decl. Ex. B ("PCLOB 702 Report") at 5, 16-20.

"[T]he agency intercepts communications directly from the Internet 'backbone'" using "NSA-designed . . . Internet collection devices [that] acquire transactions as they cross the Internet." *Id*. at 124, 39; *see also id*. at 7, 35-41. "[U]pstream collection acquires 'Internet transactions,' meaning packets of data that traverse the Internet, directly from the Internet 'backbone.'" *Id*. at 84 ("Upstream" is the NSA's present name for its Internet backbone interception technique.).

The NSA's interceptions occur "with the compelled assistance of providers that control the telecommunications 'backbone' over which . . . Internet communications transit." *Id*. at 7. The interceptions are of "communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the 'Internet backbone.' The provider is compelled to assist the government in acquiring communications across these circuits," making clear that the service providers like AT&T are the government's agent here.[8] *Id*. at 36-37.

The function of the NSA's Internet content surveillance is to intercept communications containing designated selectors. *See* PCLOB 702 Report at 7, 33, 36-37, 41. To do so, "selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through . . . the 'Internet backbone.' . . . To identify and acquire Internet transactions associated with the . . . selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions . . . ." *Id*. at 36-37. NSA uses "technical means, such as Internet protocol

[8] Other government disclosures confirm the interception of Internet backbone communications. "NSA collects electronic communications with the compelled assistance of electronic communications service providers as they transit Internet 'backbone' facilities within the United States." ECF No. 227 at 25; ECF No. 253-3, Ex. B at 3 ("NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States"); Greene Decl., Ex. B at 5 n.3 (FISC Oct. 3, 2011 Opinion); Greene Decl., Ex. C at 26 ("the acquisition of Internet communications as they transit the 'internet backbone' facilities") (FISC Sept. 25, 2012 Opinion).

('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States." *Id*. at 38; *see also id*. at 41.

The fact that the system includes filtering to exclude domestic communications proves that the circuits the government monitors contain both wholly domestic as well as international communications. Filtering would be unnecessary if the circuits did not carry wholly domestic communications, in addition to international communications, in the first instance. Experts Dr. Brian Reid and Professor Matt Blaze both confirm this point. Declaration of Dr. Brian Reid ("Reid Decl."), ¶¶ 63-64; Declaration of Professor Matt Blaze ("Blaze Decl."), ¶¶ 54-56.

That AT&T customers were included in this surveillance is evident from the government's further admission that its Internet backbone interceptions occur "in the flow of communications between communication service providers." PCLOB 702 Report at 35. AT&T is a major provider of Internet services and one of the largest Internet backbone network operators. ECF No. 89 ("Marcus Decl.") at ¶ 122; *see also* Blaze Decl. ¶¶ 26, 41. AT&T's Internet facilities in San Francisco include interconnections ("peering links") between AT&T's Internet backbone and the Internet backbones of other Internet providers. ECF No. 84-4 ("Klein Decl.") at ¶¶ 19, 22, 29-34; ECF No. 84-1 ("Russell Decl.") at ¶¶ 6, 10, 15, 19, 21, 23; Blaze Decl. ¶ 23; Reid Decl. ¶¶ 34-37. . These interconnections are where "the flow of communications between communication service providers" occurs. PCLOB 702 Report at 35.

Public documents and the first-hand accounts of the witnesses all support the fact of AT&T's involvement in this acknowledged program. This evidence amply proves AT&T's involvement; indeed, there is no evidence for the remarkable proposition that AT&T was excluded from this comprehensive surveillance scheme. The evidence is certainly sufficient to prove injury-in-fact, i.e., that the Internet communications of AT&T's customers, especially those in physical proximity to the tapping locations like Folsom Street, were more likely than not touched by this surveillance. *See* Blaze Decl. ¶ 44; Reid Decl. ¶ 51.

AT&T's documents and the first-hand participation and personal observations of AT&T employee Mark Klein show that all of the communications flowing across interconnections (peering links) between AT&T's Internet backbone network in San Francisco and other key

locations and the Internet backbones of other communications providers are copied using fiber-optic splitters. Klein Decl. ¶¶ 21-34, 36; ECF Nos. 84-3, 84-4, 84-5, 84-6 ("Klein Decl., Exs. A, B, C"); Marcus Decl. ¶¶ 56-58, 62, 70-73, 77, 109, 113-18; Russell Decl. ¶¶ 6, 10-12, 15, 19-23. The entire stream of communications copied by the splitters is then redirected and transmitted to a secure room in AT&T's facilities under the control of the NSA. Klein Decl. ¶¶ 8-10, 12, 14, 16-18, 36; Marcus Decl. ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47. Expert Dr. Reid explains and confirms that the splitters would have captured and redirected all of the Internet traffic passing through the peering-link fibers into which the splitters were installed. Reid Decl. ¶¶ 2, 20, 22, 37-41, 47; *see also* Blaze Decl. ¶¶ 34, 37.

The AT&T documents show that the AT&T secure room on Folsom Street contains equipment designed to perform the filtering and searching of the redirected copies of Internet communications described by the PCLOB, including means for scanning the contents of those communications for selectors or other search terms and means for receiving the transmission of selectors or other search terms from outside the room. Klein Decl. ¶¶ 28, 35, Ex. C; Russell Decl. ¶¶ 6, 15, 19, 22-23; Marcus Decl. ¶¶ 68, 70-77, 79-85; Reid Decl. ¶¶ 42-47. The NSA controls the operation of the AT&T secure room. Klein Decl. ¶¶ 8-10, 12, 14, 16-18, 36; Marcus Decl. ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47.

The new evidence from long-time AT&T employee Phillip Long corroborates AT&T's participation. In the mid-2000s, Long was directed to shut down existing Internet backbone connections in Northern California and instead reroute the Internet traffic those connections served to 611 Folsom Street. Declaration of Phillip Long ("Long Decl.") ¶¶ 9-20. Long explains that there was no reason from a business or engineering standpoint to route all Internet traffic through 611 Folsom Street. *Id*. at ¶¶ 15-19. These reroutings continued in existence through Long's retirement in 2015. *Id*. at 25. Long also observed the secret locked room at Folsom Street (Room 641A) where the Internet traffic copied by the splitter was sent. *Id*. at ¶ 21. Contrary to AT&T's normal engineering processes, Long was instructed to run a large fiber-optic cable to the doorstep of the AT&T secure room and connect it to a similar fiber-optic cable coming from the AT&T secure room. *Id*. at ¶ 22.

Nor are Klein and Long alone. First, AT&T's Director of Asset Protection Russell independently verified Klein's information. Russell Decl. ¶¶ 6, 10-22. And, of course, the AT&T documents verify Klein's testimony and those documents were authenticated by Russell. *Id*.; Klein Decl., Exs. A, B, C. Russell verifies that the documents *and Klein's statements* accurately describe the equipment and interconnections both inside and outside the AT&T secure room. Russell Decl. ¶¶ 6, 10-23.

Dr. Reid, an experienced network engineering expert who has first-hand knowledge of splitter technology described in Klein's declaration and the AT&T documents, explains that the technological setup Klein describes, and which Russell verifies as accurate, "passively copies all traffic passing over all of the peering-link fibers into which the splitters were installed." Reid Decl., ¶ 22(a). He notes that the splitter described is "purely optical" and that it "copies everything": it "accepts one inbound beam of light and produces two or more outbound beams of light." *Id.* at ¶¶ 22(a), 41. It "does not and cannot study the contents of a transmission to make a decision about whether to copy it"; it "does not even use electricity." *Id*. As Dr. Reid explains, "[i]t would not make sense to use an active device such as a router or switch to do inline searching of every communication routed through it because of cost and performance issues. The number of such devices needed would be in the hundreds or even thousands, and they would slow down all traffic." *Id.* at ¶ 22(b).

Dr. Reid states that given the volatile nature of Internet routing, "it is unfathomable . . . that in 17 years, at least one of plaintiffs' communications did not travel via the peering points at AT&T's 611 Folsom Street Facility, a major Internet peering point" and that it is "highly likely that plaintiffs' communications traveled through the peering links" described by Klein. *Id.* at 48. He stated that this would be true even if plaintiffs were not AT&T Internet customers, as a function of communication with AT&T customers: "Anytime a non-AT&T customer sends a communication over the internet to an AT&T customer, that communication has to pass through a peering link from another network to the AT&T network." *Id.* at 50.

Professor Blaze similarly explains that "a 'splitter,' as used in this case, is a device that optically 'splits' all communication on a link between two network nodes, creating an second link

that can be connected to a third node." Blaze Decl. ¶ 34. "This effectively copies all the traffic on the original link to the third node, while leaving the traffic undisturbed between the original two nodes." *Id.* Blaze describes the splitter as "in effect, a specialized device for physically 'wiretapping' the kinds of high-speed optical communication links that make up the Internet backbone." *Id.*

Blaze states, based on his expertise in how the Internet "routes" communications, "[i]t is highly likely that the communications of all plaintiffs passed through the link connected to the splitter (and thus the splitter itself) that Klein describes." *Id.* at 39. He notes that, pursuant to his understanding based on the available evidence, the "peering-link fibers to which the splitter was attached carried a high concentration of the international and domestic Internet traffic passing through the AT&T San Francisco facility." *Id.* at 41. "That means that the link connected to the splitter would, in turn, have access to a large fraction of the traffic passing through the facility"—which "would include Internet traffic of AT&T's customers— including traffic of plaintiffs who are AT&T Internet customers—as well as peering traffic of customers of other ISPs who communicate online with AT&T customers." *Id.* As Blaze explains, "[p]ursuant to the inherent architecture of the Internet, in order for a communication from an AT&T customer to reach a non-AT&T customer, that communication has to pass through a peering point with another network. Likewise, a communication from a non-AT&T customer to an AT&T customer must has to pass through a peering point with another network." *Id.* at 42.

The government's admissions corroborate the AT&T documents, the Klein and Long eyewitness evidence, and the testimony of experts Professor Blaze, Dr. Reid and previously, J. Scott Marcus. Those admissions describe a process that begins with "devices" "intercept[ing] communications directly from the Internet 'backbone'" with the compelled assistance of Internet backbone providers, followed by content searching of communications—the same process described by Klein and Marcus. PCLOB 702 Report at 124.

The NSA Draft OIG Report also evidences AT&T's participation in Internet content surveillance. ECF No. 147 at Ex. A at 33 (*see* footnote 6, above).

Plaintiffs are California residents, four of whom use AT&T's Internet services. Jewel Decl.

¶¶ 3-5; Knutzen Decl. ¶¶ 3-7; Walton Decl. ¶¶ 3-5; Hicks Decl. ¶ 7. The AT&T Internet backbone circuits that are copied carry the communications of plaintiffs and other AT&T customers. Marcus Decl. ¶ 108. Plaintiffs use the Internet to communicate overseas, including by engaging in email correspondences with individuals in such countries as New Zealand, Holland, Denmark, South Africa, Taiwan, Canada, France, Germany, the United Kingdom, Spain, and Saudi Arabia, as well as visiting foreign websites. Jewel Decl. ¶¶ 9-10; Knutzen Decl. ¶ 11; Walton Decl. ¶¶ 9, 18; Hepting Decl. ¶¶ 16-17. So even if the initial copying and redirection by the splitters or other technology were somehow limited to only international communications, plaintiffs' communications still would have been copied and redirected.

Whatever filtering and scanning occurs after the bulk copying and redirection that Klein witnessed does not affect plaintiffs' standing. Even if the filtering eliminates plaintiffs' communications before the scanning occurs, plaintiffs nonetheless have standing because of the initial copying and redirection of their communications.

Moreover, even if it were the case that plaintiffs' communications were never filtered or scanned, e.g., if the devices Klein operated were solely for the purpose of gathering Internet metadata like "to" and "from" email addresses, the initial copying and redirection of the entire communication, including its contents, would still give rise to a Wiretap Act claim for communications acquisition, and plaintiffs would have standing. This is because in order to collect the "to" and "from" addresses of an email, it is necessary to acquire and examine the entire contents of the email because that is where the addresses reside. *See* Blaze Decl. ¶¶ 22, 27, 38 ("Given the inherent structure of the Internet outlined above, there is no way to view or collect the 'to' and 'from' addressing information from an email messages by packet interception without first reconstructing the email message content by reassembling the contents of all of the relevant packets."); Reid Decl. ¶¶ 22(c), 59-61.

And as expert Ashkan Soltani explains, a surveillance network with the features admitted by the government would also very likely intercept the communications of users of cloud-based applications such as webmail like Google's Gmail and Yahoo mail. Soltani Decl. ¶ 16. That is because providers of these applications have established databases that automatically move users'

communications in "shards" between data centers around the world "specifically to traverse geographic borders in order to provide geographic redundancy." *Id.* The movement of user communications shards happens without user action such as sending or receiving an email, and interception of even a single shard would allow the NSA or other outsider to glean significant information about the communication's contents. *Id.* ¶¶ 19-24. Plaintiffs Jewel, Hepting, Knutzen, and Walton are Gmail users, while Jewel, Knutzen, and Walton are Yahoo users. Jewel Decl. ¶¶ 16, 19; Hepting Decl. ¶ 12; Knutzen Decl. ¶¶ 14, 15; Walton Decl. ¶¶ 15, 17.

Drawing all inferences in plaintiffs' favor, a rational factfinder could easily conclude that it is more probable than not that at least one of each plaintiffs' Internet communications have been copied and redirected. In order to deny plaintiffs standing, the Court would have to find that since 2001 not a single one of plaintiffs' many Internet communications, both international and domestic, is likely to have passed over the Internet backbone peering connections between providers where the government copied and redirected communications for further filtering and scanning, including the peering connections at 611 Folsom Street. Given the scope and system of interception created by the government, such a finding would be in error.

2. The Court's previous ruling that plaintiffs lack standing for their Fourth Amendment Internet interception claims was mistaken.

The Court previously concluded that plaintiffs lacked standing to pursue their Fourth Amendment Internet interception claim. That ruling was mistaken.

Plaintiffs' motion did not "allege that, as AT&T customers, *all* of their Internet communications have been collected *and amassed in storage*," as the Court mistakenly believed. ECF No. 321 at 6 (italics added). Plaintiffs challenged only the initial copying, redirection, and searching of their communications, not storage. They stated that whether or not the government ultimately put in storage any of their communications was irrelevant to their Fourth Amendment claim. ECF No. 261 at 8-9 ("The communications the government retains at stage four [of plaintiffs' diagram at p. 5, the storage stage] are not at issue here.").

Plaintiffs also did not claim that "*all*" of their communications were intercepted. They did not need to. Standing requires only a single interception for each of them. Even accepting the

government's claim that the surveillance was aimed at international communications, a reasonable likelihood of interception is easy to find, since plaintiffs regularly engage in international Internet communications. Jewel Decl. ¶¶ 9-10; Knutzen Decl. ¶ 11; Walton Decl. ¶¶ 9, 18; Hepting Decl. ¶¶ 16-17.

On the law, the Court was mistaken in requiring plaintiffs to show more than the initial mass interception to establish their standing. While faulting the sufficiency of plaintiffs' showing as to what occurs in the AT&T secure room *after* the initial copying and redirection of plaintiffs' communications by the fiber-optic splitters outside of the secure room, the Court did not dispute that plaintiffs' eyewitness evidence was sufficient to establish the initial copying and redirection by the splitters. ECF No. 321 at 8. That evidence is also supported by the government's admissions that communications are intercepted by devices sitting on the Internet backbone, before any filtering or scanning or storage occurs. PCLOB 702 Report at 36-37, 39, 124. . The Long Declaration and the expert witness conclusions of Dr. Reid, Professor Blaze, and Soltani now buttress this evidence. Reid Decl. ¶¶ 20-24, 47, 48-51, 55-58, 63-64; Blaze Decl. ¶¶ 11-14, 39, 41-46, 51, 55-57; [Soltani Decl. ¶ X].

But that initial copying and redirection—not permanent storage—is all plaintiffs needed to show to establish standing. By requiring plaintiffs to show more, *i.e.*, to show what happened after the injury-in-fact caused by the initial copying and redirection, the Court erroneously strayed from "the threshold standing determination." *Jewel*, 673 F.3d at 911 n.5.

The Court also improperly disregarded the testimony of Klein, Marcus, and Russell, and ignored the AT&T documents, erroneously concluding that "Klein cannot establish the content, function, or purpose of the secure room" or "what data were actually processed and by whom in the secure room." ECF No. 321 at 8. But Klein has personal knowledge of the only thing that matters for standing: he knows what was copied by the splitters and "what data were actually processed . . . in the secure room" (*id.*) because he was in charge of the devices copying AT&T's Internet backbone communications and transmitting the copies to the AT&T secure room over fiber-optic cables. Klein Decl. ¶¶ 15, 27, 34. As directed by the AT&T documents he relied upon to do his job, he physically connected Internet backbone circuits to the splitters he operated, and he

describes in detail the circuits connected to the splitters and the types of data they carry. Klein Decl. ¶¶ 19, 22, 25, 26, 28-34, 36 & Exs. A, B, C. What happened *after* the initial copying and redirection Klein personally observed is irrelevant to standing.

Further, the Court disregarded entirely Russell's authentication of the AT&T documents and verification of the truth of Klein's testimony. Russell Decl. ¶¶ 6, 10-11, 15, 17, 19-23.

Klein explains the NSA's control of and involvement with the AT&T secure room. Klein Decl. ¶¶ 8-10, 12, 14, 16-18. Klein learned these facts in the course and scope of his employment, making them admissible. *U.S. v. Neal*, 36 F.3d 1190, 1206 (1st Cir. 1994). And the statements by other AT&T employees are admissible non-hearsay. Fed. R. Evid. 801(d)(2)(D), 803(3) .

The Court erroneously discounted Marcus's expert testimony, mistakenly believing that "Marcus relies exclusively on the observations and assumptions by Klein." ECF No. 321 at 8. Marcus's testimony, however, is based not just on Klein's testimony, but also on the AT&T documents and other independent evidence Marcus cites and on Marcus's decades of knowledge and personal experience in telecommunications, including providing Internet backbone services to AT&T. Marcus Decl. ¶¶ 7, 13-18, 24, 27, 29. Marcus independently concluded that government surveillance is the purpose of the equipment Klein describes, without relying on any of Klein's statements regarding the NSA's participation and without relying on any "assumed operational details" (ECF No. 321 at 8). Marcus Decl. ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47. Marcus's testimony about the "purpose and function of the secure equipment at AT&T" (ECF No. 321 at 8) is based on the AT&T documents showing the existence of that equipment in the AT&T secure room (a fact confirmed by Russell) and on his independent expert knowledge about the capabilities of that equipment. Marcus Decl. ¶¶ 67-68, 70-77, 79-85.

C. Internet Metadata

The evidence demonstrates that it is more likely than not that since 2001 at least one Internet metadata record of an Internet communication by each plaintiff was obtained by the government, which is all that plaintiffs need show to establish an injury-in-fact.

The bulk collection of Internet metadata began in 2001. PCLOB 215 Report at 37-40. The NSA Draft IG report confirms that AT&T and Verizon participated in the Internet metadata

program. ECF No. 147, Ex. A at 34, 38-39 (*see* footnote 4 above).

Like the phone records program, it, too, was a broad-based collection program. PR/TT Order at 115 (describing government's Internet metadata collection as "massive"). It, too, was a contact-chaining program that needed to collect metadata from extremely large numbers of communications to be successful. In the FISC's words, to contact-chain the communications of suspected terrorists required "'the collection of both a huge volume and a high percentage of unrelated communications.'" PR/TT Order at 9.

And, over time, the Internet metadata program expanded "to acquire a much larger volume of metadata at a greatly expanded range of facilities." PR/TT Order at 71. It was no longer limited to "streams of data with a relatively high concentration of Foreign Power communications" but was "wholly non-targeted bulk production." PR/TT Order at 74. This "11- to 24-fold increase in volume" correspondingly resulted in "captur[ing] metadata for a larger volume of U.S. person communications." PR/TT Order at 72, 75 n.61.

The government's position is that Internet metadata bulk collection focused on only certain categories of communications (including email metadata) and on international communications channels. PCLOB 215 Report at 37-39, 44; ECF No. 147, Ex. A at 34, 37-39; PR/TT Order at 71, 81, 108. Even that resulted in the collection of trillions of Internet metadata records per month. Wiebe Decl., Ex. G. Yet even assuming that Internet metadata collection was limited to international communications, plaintiffs regularly send international emails and engage in other international communications. Jewel Decl. ¶¶ 9-10; Knutzen Decl. ¶ 11; Walton Decl. ¶¶ 9, 18; Hepting Decl. ¶¶ 16-17. It is certainly more likely than not that one of the plaintiffs' email had its metadata collected by this program. Indeed, the notion that not a single one of their international emails was ever snared in the mass Internet metadata collection processes is highly improbable.

Moreover, despite the government's assertions about the *intended* limitations on Internet metadata collection, the FISC found that throughout the program's existence it systemically overcollected Internet metadata far beyond the limitations imposed by the FISC's orders. PR/TT Order at 3 ("NSA exceeded the scope of authorized acquisition continuously"), 9, 20 ("systemic overcollection"). NSA's violations of the FISC orders were "longstanding and pervasive." PR/TT

Order at 115. NSA's overcollection was "sweeping and non-targeted." PR/TT Order at 110. "[T]his continuous overcollection acquired many other types of data" not authorized by the FISC and "'[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection." PR/TT Order at 20-21. NSA's reporting on the Internet metadata program to the FISC was rife with misrepresentations. PR/TT Order at 11, 14-22, 72; Greene Decl., Ex. B at 16-17 n.14 (FISC Oct. 3, 2011 Opinion).

As experts Professor Blaze and Dr. Reid both explain in their declarations, because of the inherent architecture of the Internet, the government cannot even collect [what it calls] metadata—e.g., the "to", "from", and subject line information information—"without first reconstructing the email message content by reassembling the contents of all of the relevant packets." *See* Blaze Decl. ¶¶ 22, 27, 38. Reid Decl. ¶¶ 22(c), 59-61. As Professor Blaze explains, "[t]he outdated conception of a bright line between content and addressing information (which is sometimes referred to as "metadata") originates from early phone networks"—where there was a clear line between "dialing, routing, addressing, and signaling (DRAS) information" used by the phone companies and the content of calls. Blaze Decl. ¶ 28. On the Internet, the various layers an email must travel through "all have their own identifiers—and none of these identifiers include the email address listed in the 'to' or 'from' fields in an email." *Id.* at ¶ 33. "From a technical perspective, the 'to' and 'from' information, along with the subject line and the text within the body email, is all content information, because" it "can only be viewed at the application layer, after content has been extracted and reassembled from the relevant packets." *Id.*

Indeed, as the expert declaration of Soltani confirms, even a surveillance program directed solely at foreign communications would likely intercept purely domestic communications of users of cloud-based applications like plaintiffs. Soltani Decl. ¶ 25.

As with the bulk collection of call records and the mass interference with Internet communications, a rational factfinder drawing all inferences in plaintiffs' favor could conclude that it is more probable than not that at least one of each plaintiff's Internet metadata records has been collected.

III. The Undisclosed Classified Evidence Also Demonstrates Plaintiffs' Standing

The Court has required plaintiffs to direct it to the evidence that gives them standing from the public record. Plaintiffs have done so, and this public evidence alone is sufficient to prove plaintiffs' standing. In addition, plaintiffs are confident that the undisclosed classified evidence includes the following categories of additional evidence supporting plaintiffs' standing.

Classified Evidence	Phone Records	Internet Content	Internet Metadata
Letters from the Attorney General or other government officials to plaintiffs' communications providers during President's Surveillance Program showing participation of plaintiffs' phone and ISP providers in phone records, Internet content, and Internet metadata programs.	X	X	X
Post-PSP FISC Orders showing participation of plaintiffs' phone and ISP providers in phone records, Internet content, and Internet metadata programs.	X	X	X
Government documents illustrating or describing Internet backbone surveillance activities showing Internet content and metadata was collected by copying and filtering Internet transmissions at peering points and other major Internet backbone nodes, including AT&T's.		X	X
The presence of plaintiffs' phone numbers in the phone records retained by the government.	X		
The presence of plaintiffs' Internet identifiers in the Internet metadata retained by the government.			X
Unredacted versions of FISC opinions.	X	X	X
Authentication of the documents designated in plaintiffs' RFAs, including the NSA OIG Report, the exhibits to the Klein declaration, and Wiebe Decl., Exs. H, I.	X	X	X
Evidence establishing that "Fairview" is a codeword designating AT&T's participation in the programs at issue and "Stormbrew" is a codeword designating Verizon's participation in the programs at issue.	X	X	X
Documents, including diagrams, evidencing the participation in the programs at issue by AT&T (including under the name "Fairview") and Verizon (including under the name "Stormbrew").	X	X	X

If the classified evidence confirms that plaintiffs have standing, then plaintiffs have

standing. The Court ordered the government to provide it with all evidence of standing and authorized plaintiffs to propound discovery requests on the issue. The government has responded, albeit in way that has barred plaintiffs from access to its substantive responses. Assuming that the government provided its discovery responses in good faith, the Court has before it classified evidence establishing plaintiffs' standing, both directly and circumstantially. The government's responses might be classified, but that does not mean that the Court may not rely on them to determine standing. Indeed, the Court has a duty to do so. If the Court were to refuse to even consider the classified evidence, that would derogate Congress' intent in enacting sections 2712 and 1806(f) to hold the government accountable for the legality of its surveillance.

In particular, given the vast volume of phone records and Internet metadata in the government's databases, plaintiffs expect that the government found their phone numbers and Internet communications identifiers when it searched those databases as the Court required. That is conclusive evidence of standing for those two programs.

Moreover, despite the existence of formal preservation orders, the government has plainly breached its evidence preservation duties. It admittedly destroyed all phone records from May 2006 to sometime in 2009 and destroyed all Internet metadata from 2004 to the program's end in December 2011. ECF No. 260 at 9. The government now possesses phone records only from October 2001 to May 2006 and from sometime in 2009 to the program's end in November 2015. ECF Nos. 230 at ¶ 39; 228 at ¶ 31. It possesses Internet metadata only from October 2001 to July 2004. ECF No. 230 at ¶ 38.

If the government did not find plaintiffs' identifiers in its currently held databases, the Court should impose an evidentiary spoliation sanction that takes as established that plaintiffs' identifiers were present in the phone records and Internet metadata the government destroyed during the pendency of this action and the overlapping *Hepting* action when it was subject to evidence preservation orders. *See* ECF Nos 367, 373.

IV. Section 2712(b)(4) Requires The Use Of Classified Evidence To Decide Standing

A. Section 2712 governs the use of classified evidence here.

Section 2712 was enacted as part of the USA PATRIOT Act in October 2001. Pub. L. No.

107-56, 115 Stat. 272. The USA PATRIOT Act expanded the government's national security surveillance powers. Section 2712 was enacted to provide judicial review of any abuse of those powers by creating a civil remedy against the government for Wiretap Act and SCA violations. Congress recognized that classified evidence would often be relevant and necessary in section 2712 lawsuits, and intended that such evidence be used to decide issues on their merits, not excluded. For that reason, it preempted the state secrets privilege with section 2712(b)(4), as the Court has held. ECF Nos. 347 at 1-2; 340 at 2; *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1105 (N.D. Cal. 2013).

Section 2712(b)(4) makes the procedures of section 1806(f) the "exclusive means" governing classified materials "[n]otwithstanding any other provision of law," including for purposes of standing. Section 2712(b)(4) is broader than section 1806(f); section 1806(f) creates a procedure for using classified evidence *ex parte*, *in camera* to decide whether surveillance is lawfully authorized and conducted. Section 2712(b)(4) directs that those same *ex parte*, *in camera* procedures are the "exclusive means by which [classified materials] . . . may be reviewed" for *any* purpose—which includes determinations of standing.

Plaintiffs meet the test of section 2712(b)(4) because the government has produced classified materials in response to plaintiffs' discovery requests and has asserted that "disclosure . . . would harm the national security" (§1806(f)), meaning that those materials are "materials governed by" section 1806(f) that section 2712(b)(4) in turn requires the Court to review *ex parte* and *in camera* to decide the issues in this lawsuit.

Plaintiffs thus are entitled to have the Court use the classified evidence *ex parte* and *in camera* to determine their standing. The government's arguments against doing so are the same ones the Court previously rejected here and in the related MDL litigation *In re NSA Telecom. Records Litigation*, 595 F. Supp. 2d 1077, 1085 (N.D. Cal. 2009).

B. Plaintiffs have met any possible test for using section 1806(f)'s procedures.

In any event, plaintiffs have met any other threshold for using 1806(f)'s procedures that the Court may adopt. First, plaintiffs have met the test for using section 1806(f) this Court adopted and applied in the related *In re NSA* MDL. 595 F. Supp. 2d at 1085. The Court held that "*proof* of plaintiffs' claims is not necessary at this stage." *Id*. (italics original). Instead, all that is required

are "allegations [that] 'are sufficiently definite, specific, detailed, and nonconjectural, to enable the court to conclude that a substantial claim is presented.' " *Id*. As *In re NSA* explains, once a plaintiff does so, she may use section 1806(f) to prove up standing. *Id*. at 1085-88.

Plaintiffs have far exceeded this test, for not only have they alleged substantial claims (as the Ninth Circuit held, 673 F.3d at 910) that are definite, specific, detailed, and nonconjectural, they have gone beyond that standard with the public evidence demonstrating they were surveilled.

Second, if proof of standing is the test for using section 1806(f), plaintiffs have met that as well by demonstrating injury-in-fact using the public evidence.

C. Plaintiffs are aggrieved persons.

Plaintiffs also meet the test of "aggrieved person," even though that is not the test that section 2712(b)(4) imposes.

The Court should reject these arguments now just as it did the government's identical arguments in 2009 in *In re NSA MDL*, 595 F. Supp. 2d at 1083-88. The government's argument that classified evidence cannot be used under section 2712(b)(4) unless plaintiffs first prove they are aggrieved persons is contrary to the will of Congress and the law of the case. The Ninth Circuit has held that whether plaintiffs are aggrieved persons "is a merits determination, not a threshold standing question." *Jewel*, 673 F.3d at 907 n.4. In section 2712 cases, Congress has dictated that merits determinations must be made using classified evidence reviewed *ex parte*, *in camera*, i.e., using the "procedures of section 106(f) [i.e., section 1806(f)]." § 2712(b)(4). Because aggrieved-person status is a merits determination, it thus must be determined using classified evidence reviewed *ex parte*, *in camera*.

In any event, plaintiffs are in fact "aggrieved persons." As the government's authority explains, a person is aggrieved if her claim falls within the "zone of interests" of a statutory cause of action. *Dir., Office of Workers' Comp. Prog. v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 127 (1995). This is a question of statutory standing (sometimes called prudential standing, although the Supreme Court is moving away from using either term), not Article III standing. *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 125-32 & nn. 3-4 (2014); *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 19-20 (1998) (applying zone-of-interests test

to aggrieved-person determination). The Ninth Circuit addressed this point in the prior appeal. *Jewel*, 673 F.3d at 907 n.4, 912-13. It is law of the case that plaintiffs have prudential standing and have satisfied the "zone of interests" test, thus establishing that they are aggrieved persons: "[Plaintiffs'] statutory claims undoubtedly allege harms 'within the zone of interests to be protected or regulated by the statute[s],' alleviating any prudential standing concerns." *Id*. at 913.

Other routes of analysis also lead to the conclusion that plaintiffs are aggrieved persons. An "aggrieved person" under section 2712 is simply a person with allegations of unlawful surveillance adequate to support a complaint, i.e., someone within the zone of interests of the Wiretap Act and the SCA: "Any person who is aggrieved by any willful violation of this chapter or of chapter 119 . . . may commence an action . . . ." § 2712(a). Section 2712(a) goes on to describe the remedies available "if a person who is aggrieved successfully establishes such a violation." *Id*. In doing so, section 2712(a) clearly distinguishes someone "who is aggrieved" because he or she has allegations sufficient to "commence an action" from someone who has gone on to "successfully establish[]" a violation. *Id*. Plaintiffs are aggrieved persons under section 2712 because their allegations are more than sufficient to commence an action.

Plaintiffs are "aggrieved persons" under section 1806(f) as well. Under FISA, an "aggrieved person" is simply "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Congress' intent in creating the "aggrieved person" standard was not to limit the operation of section 1806(f) but to make FISA's substantive remedies "coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance." H.R. Rep. No. 95-1283, at 66 (1978) (ECF No. 90, Ex. I). The purpose of the "aggrieved person" definition was simply to exclude from FISA's remedies those who were not parties to the intercepted communication, because Congress "no intent to create a statutory right in such persons." *Id*.

In section 1806(f), "aggrieved person" is merely a description of a person with an unlawful surveillance claim who makes a discovery request. A plaintiff may propound discovery without first proving up standing or the merits. It is *not* the plaintiff's discovery request but the

government's assertion that classified evidence is at issue that triggers section 1806(f)'s procedures. § 1806(f). "The special procedures . . . cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security . . . . If no such assertion is made, the committee envisions . . . mandatory disclosure . . . ." S. Rep. No. 95-701, at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 (ECF No. 90, Ex. J); H.R. Conf. Rep. No. 95-1720, at 32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061 (same) (ECF No. 90, Ex. G).

It is thus the government, not the plaintiff, that triggers section 1806(f), the plaintiff does not have to prove anything to trigger its operation. Unless the government asserts that classified evidence is at issue, discovery continues along its ordinary course, evidence is disclosed, and section 1806(f) never comes into play. If the government makes the assertion, then the Court must use the classified evidence to decide the case.

Ultimately, the government's position is that in section 2712(b)(4) Congress intended its incorporation of section 1806(f)'s procedures to erect a barrier to litigating electronic surveillance claims, rather than to create the means for making litigation of those claims feasible. Exactly the opposite is the case, as this Court has held. *Jewel*, 965 F. Supp. 2d at 1103-06. Congress did not enact section 2712 to create claims that no one could ever litigate.

D. The government's definition of "aggrieved person" is erroneous; nevertheless Plaintiffs meet it.

The government's "aggrieved person" argument fails for another reason; it mischaracterizes "aggrieved person" as someone who has proven up the fact of surveillance. In doing so, it essentially equates "aggrieved person" with Article III standing. That is contrary to the established meaning of "aggrieved person" as someone who falls within the zone of interests of a statute, and is contrary to the law of the case here. *Jewel*, 673 F.3d at 907 n.4, 912-13. In any event, plaintiffs meet even the government's misconceived definition of "aggrieved person" because in showing their injury-in-fact they have established the fact of surveillance.

E. *Wikimedia* is inapposite, and plaintiffs satisfy its test.

In *Wikimedia v. NSA/CSS*, 2018 WL 3973016 (D. Md. Aug. 20, 2018), the court held that to

trigger section 1806(f) "a plaintiff must first adduce evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance." *Id*. at *8. *Wikimedia* has no persuasive authority here. Foremost, it is not a section 2712 case and does not speak to section 2712(b)(4). Second, *Wikimedia* rejects this Court's holding in the related *In re NSA* MDL as to the proper standard for applying section 1806(f). *Id*. at *9-10. Third, plaintiffs have adduced evidence far beyond what is needed to show that there is at least a genuine dispute as to whether they have been subjected to electronic surveillance, the *Wikimedia* standard.

F. This Court must reject the government's attempt to undermine the Court's holding that sections 2712(b)(4) and 1806(f) preempt the state secrets privilege.

In 2013, the Court granted partial summary judgment for plaintiffs and ruled that sections 2712 and 1806(f) preempt and displace the state secrets privilege and the government's statutory privileges in electronic surveillance case: "[T]he Court GRANTS the Jewel Plaintiffs' motion for partial summary adjudication by rejecting the state secrets defense as having been displaced by the statutory procedure prescribed in 50 U.S.C. § 1806(f)." *Jewel*, 965 F. Supp. 2d at 1097; *id*. at 1112 (same); ECF No. 347 at 1-2; ECF No. 340 at 2. Acting at the specific direction of the Ninth Circuit to decide this issue (673 F.3d at 913-14), the Court found:"as a matter of law, the FISA procedural mechanism prescribed under 50 U.S.C. § 1806(f) preempts application of the state secrets privilege." *Id*. at 1103.

But even apart from that bar, the government's argument still lacks merit for all the many reasons the Court found in its 2013 order and that plaintiffs have set forth over the years. *See, e.g.,* ECF Nos. 29; 38-1; 83; 90; 112; 131; 140; 177; 203; 294-3; 401; 407. Plaintiffs note two.

First, the government's argument fails to address section 2712. Congress created a civil remedy for unlawful surveillance in section 2712(a) and expressly mandated in section 2712(b)(4) that the section 1806(f) procedures were the "exclusive means" for handling classified materials "[n]otwithstanding any other provision of law." By doing so, section 2712(b)(4) expressly preempted the state secrets privilege, as the Court has repeatedly found. "The Court . . . specifically found that section 2712(b)(4) 'designat[es] Section 1806(f) as "the exclusive means by which materials [designated as sensitive by the government] shall be reviewed" in suits against the

United States under FISA, the Wiretap Action, and the Electronic Privacy Protection Act.'" ECF No. 340 at 2 (brackets original); *accord* ECF No. 347 at 1-2; *Jewel*, 965 F. Supp. 2d at 1105.

Second, the legislative history rebuts the government's contention that section 1806(f) applies only in criminal cases where the government seeks to use surveillance evidence. In section 1806(f)'s legislative history, Congress stated that section 1806(f)'s procedures are "appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases" (H.R. Conf. Rep. No. 95-1720, at 32, 1978 U.S.C.C.A.N. at 4061 (ECF No. 90, Ex. G) and that use of section 1806(f) can be triggered by "a discovery motion in a civil trial" (H.R. Rep. No. 95-1283, at 93 (1978) (ECF No. 119-1)).

So holds the law of this case: "Based on the legislative history and the plain language of FISA, this Court finds that FISA preempts the common law doctrine of the state secrets privilege." *Jewel*, 965 F. Supp. 2d at 1105. In any event, section 2712 expressly broadened section 1806(f)'s use to plaintiffs bringing Wiretap Act and SCA civil claims against the government.[9] *Id*.

V. This lawsuit may not be dismissed on state secrets grounds.

A. Congress has precluded any state secrets dismissal of this lawsuit.

By enacting section 2712, Congress preempted any use of the state secrets privilege to dismiss this lawsuit. It did so both by creating claims against the government for abuses of (inherently secret) national security surveillance and by creating procedures for using secret evidence to decide those claims.

The Court nevertheless suggests that even if plaintiffs can prove their claims without classified evidence, or alternatively, even if they have satisfied any preconditions under section 2712(b)(4) for using the procedures of section 1806(f), it may dismiss plaintiffs' claims if it determines that "litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (en banc). *See* ECF No. 410 at 2.

[9] In the cross-motions the Court decided in 2013, the government raised and the Court rejected the 50 U.S.C. §§ 3024(i)(1), 3605(a) statutory privileges. *Jewel*, 965 F. Supp. 2d at 1097 (referencing "the statutory protections . . . asserted in this action"). The government raises them again now, but there is no ground for reconsidering the Court's previous rejection. *See* ECF No. 401 at 12-15.

That would be an erroneous application of *Mohamed*. *Mohamed* holds 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. 614 F.3d at 1092 & n.15 (citing section 1806(f) as an example of such a statutory scheme). That is exactly what Congress did in section 2712, creating causes of action and the procedures to litigate them, including procedures for using classified evidence. *Mohamed* itself thus forecloses any dismissal on state secrets grounds here. Moreover, the Supreme Court's later holding in *General Dynamics v. U.S.*, 563 U.S. 478 (2011), effectively overruled the Ninth Circuit's holding in *Mohamed* and limited *Reynolds* to only the exclusion of evidence. *See* ECF No. 83 at 10-11; No. 112 at 14-16.[10]

The government makes passing reference to *Clapper v. Amnesty Int'l*, 568 U.S. 398 (2013). *Clapper* was a standing case, not a state secrets case, a section 2712(b)(4) case, or a section 1806(f) case. *See* ECF Nos. 401; 203; 177. *Clapper* was also not a mass surveillance case like *Jewel*, and its footnote 4 dicta addressed a risk unique to targeted-surveillance challenges: the risk that pursuing the lawsuit would reveal whether the plaintiff "was on the list of surveillance targets." *Clapper*, 568 U.S. at 412 n.4. Plaintiffs are pursuing claims of untargeted mass surveillance; they and the Court do not need to know who was on the list of surveillance targets for them to prove their claims, and a judgment in their favor will not reveal whether they or anyone else is or is not on the list of surveillance targets. In any event, as the Court and the Ninth Circuit have held, in sections 2712(b)(4) and 1806(f) Congress has struck a balance that the Court must obey. *Mohamed*, 614 F.3d at 1092 & n.15; *Jewel*, 965 F. Supp. 2d at 1105.

B. Even if the state secrets privilege governed here, the issue of standing can be safely litigated without disclosing state secrets.

Even assuming the state secrets privilege and *Mohamed* governed here, they would not bar litigation of plaintiffs' standing.[11] As both the Court and *Mohamed* recognize, the function of the

[10] Plaintiffs thus disagree with *Mohamed's* holding that *U.S. v. Reynolds*, 345 U.S. 1 (1953) permits dismissal of a lawsuit rather than just the exclusion of evidence, and preserve their right to challenge it on appeal. ECF No. 83, 112.

[11] Under *Reynolds*, the state secrets privilege may only be invoked by the relevant "head of the department." 345 U.S. at 7-8. The NSA is a unit of the Department of Defense, and the relevant

state secrets privilege is to exclude specific items of privileged evidence. *Mohamed*, 614 F.3d at 1082. The case goes on notwithstanding the exclusion of secret evidence.

This lawsuit should go on because it can be litigated without creating "an unacceptable risk of disclosing state secrets." *Mohamed*, 614 F.3d at 1083. The very subject matter of this lawsuit is not a state secret. *Jewel*, 965 F. Supp. 2d at 1102-03. The phone records program, the Internet metadata program, and "about" searching of Internet content have all currently ceased. The public evidence is extensive. The government long ago waived any state secrets privilege in any of the information in the Klein and Marcus declarations and the AT&T documents. *See Hepting v. AT&T*, 439 F. Supp. 2d 974, 989 (N.D. Cal. 2006); ECF No. 295, Ex. C.

The participation of the telecommunications companies in the government's surveillance is no secret. "AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content." *Hepting*, 439 F. Supp. 2d at 991-92. The participation of AT&T, Verizon, and Sprint in the phone records program is public. Wiebe Decl., Ex. B. And AT&T and Verizon admit in their transparency reports that they provide communications content and communications records to the government under FISA orders. Wiebe Decl., Ex. C at 3, Ex. D.

Moreover, the details of the government's surveillance methods do not need to be revealed to decide whether the fundamental rights of Americans have been infringed by the government's mass surveillance programs, which admittedly are designed to sweep up a tremendous number of the innocent along with the government's targets. The identities of the government's actual surveillance targets are irrelevant to any issue in the lawsuit and can remain safely secret.

A crucial distinction between *Mohamed* and *Jewel* is the mass surveillance nature of the case. The plaintiffs in *Mohamed* were targeted by the government for rendition to countries where they were tortured, putting at issue the factual basis on which they were targeted. Similarly, in a targeted-surveillance lawsuit, there is a risk that a determination of standing may reveal who the government has targeted for surveillance. Here, there is no such risk, because finding that

---

head of department is the Secretary of Defense. Because he has not asserted the state secrets privilege, it has not been properly invoked, as plaintiffs have explained. ECF No. 112 at 27.

plaintiffs have been subjected to mass surveillance, along with hundreds of millions of other nonsuspect Americans, says nothing about whom the government has targeted or the secret facts it has relied on in targeting.

Finally, the European Court of Human Right's recently concluded adjudication, finding certain United Kingdom bulk fiber optic surveillance regimes to be illegal, is instructive in several respects.[12]

First, the ECHR demonstrated that it is possible to rule on the lawfulness of terrorism-related bulk surveillance programs while accommodating national security concerns. And of particular note, the ECHR found the NSA's Upstream program to be "a bulk interception scheme similar to the section 8(4) regime," the UK program at issue in that case.[13]

Second, the litigation shows that in other parts of the world, some technical details of current state surveillance of fiber optic Internet communications are common knowledge. The UK government, while "neither confirming, nor denying" much of the detail, still provided the ECHR with information about how fiber optic cables are made up of multiple bearers;[14] that certain bearers are identified and their entire contents intercepted before only a "tiny proportion" of those communications are "examined";[15] that in both the US and UK programs, "strong selectors" are applied at an early stage giving each program "the flavour of targeted capabilities";[16] and why it was technologically impossible to conduct targeted surveillance without first intercepting the entire

---

[12] *Big Brother Watch And Others v. The United Kingdom* (Nos. 58170/13, 62322/14 and 24960/15) (Eur. Ct. H.R. Sept. 13, 2018), *available at* http://hudoc.echr.coe.int/eng?i=001-186048.

[13] *Id.* at p. 152 ¶ 395. As the UK government submitted to the ECHR, "although the powers under FISA s.702 do concern 'bulk interception' the powers are focused and targeted and bear a strong resemblance to GCHQ's 'strong selector' process." *Ten Human Rights Organisations and The United Kingdom* (No. 24960/15), Further Observations of the Government of the United Kingdom, ¶ 40 (Eur. Ct. H.R. Dec. 16, 2016) ("Further Observations") (Greene Decl. Exh. D), at p. 17 ¶ 40, quoting *Report on the Bulk Powers Review*, David Anderson, Q.C., Independent Reviewer of Terrorism Legislation (August 2016) (Greene Decl. Exh. E)), at §§ 3.56-3.65.

[14] First published in *Privacy And Security: A modern and transparent legal framework,* Intelligence and Security Committee of Parliament, 12 March 2105, at 26 n. 48. Greene Decl. Exh. F.

[15] "Further Observations" (Greene Decl. Exh. D) at p. 2 ¶ 7.

[16] "Further Observations" (Greene Decl. Exh. D) ¶ 40, quoting *Report on the Bulk Powers Review* (Greene Decl. Exh. E) at §§ 3.56-3.65.

contents of several bearers within a fiber optic cable.[17]

If this much information is common knowledge about current practices, similar detail about past practices cannot justify a substantive bar under the state secrets privilege.

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: September 28, 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
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

[17] *Ten Human Rights Organisations and The United Kingdom* (No. 24960/15), The United Kingdom's Observations on the Merits, (Eur. Ct. H.R. Apr. 18, 2016) (Greene Decl. Exh. G) at p. 45 ¶ 1.29(1),(2).