CASE NO. 19-16066

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (AS EXECUTRIX OF THE ESTATE OF GREGORY HICKS), AND JOICE WALTON,

PLAINTIFFS-APPELLANTS,

V.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, NO. 08-CV-04373-JSW
THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE, PRESIDING

APPELLANTS' OPENING BRIEF
Provisionally UNDER SEAL

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
PHILIP J. TASSIN
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKEY
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Rules

Legislative Materials

Other Authorities

INTRODUCTION

For over a decade, plaintiffs have sought a determination of whether the government's acknowledged mass surveillance of the Internet communications and telephone records of hundreds of millions of Americans violates the Constitution and federal statutory law. But the district court refused to do so, defying Congress's express command that such claims be decided on the merits—a command recently confirmed by this Court. *Fazaga v. FBI*, 916 F.3d 1202, 1230-38 (9th Cir. 2019).

The district court's refusal, resting on the state secrets privilege, directly contradicts this Court's instruction in *Fazaga* that Congress has preempted the state secrets privilege in electronic surveillance cases. This error must be reversed.

The district court's dismissal hands the keys to the courthouse to the Executive, making it impossible to bring any litigation challenging the legality of such surveillance without the Executive's permission. It blinds the courts to what the Executive has admitted: the NSA has engaged in mass surveillance of domestic communications carried by the nation's leading telecommunications companies, and this surveillance touches the communications and records of millions of innocent Americans.

At stake are the statutory and constitutional bulwarks created to protect "the privacies of life" from the prying eyes of an all-seeing government. *Carpenter v. U.S.*, __ U.S. __, 138 S. Ct. 2206, 2214 (2018) (citation omitted). From the founding of the Republic, the Executive's

power to surveil has required robust constitutional and statutory limitations—including searching judicial review of the legality of surveillance—to ensure the privacy and freedom of all Americans.

One important bulwark imposed by Congress is the guarantee of merits review. Indeed, Congress assured merits review twice: In section 1806(f) of the Foreign Intelligence Surveillance Act (FISA), passed in direct response to widespread misuse of electronic surveillance by the Executive in the 1970s, Congress requires the judiciary to determine whether domestic surveillance conducted for national security is "lawfully authorized and conducted," using secure *ex parte, in camera* procedures to protect state secrets. 50 U.S.C. § 1806(f) ("section 1806(f)"). In the USA PATRIOT Act, Congress reaffirmed and extended the reach of section 1806(f). 18 U.S.C. § 2712(b)(4) ("section 2712(b)(4)").

In *Fazaga*, this Court held that section 1806(f) must be construed consistent with Congress' intent to subject domestic electronic surveillance done for national security purposes to judicial oversight, thus affirming that section 1806(f) preempts the common-law state secrets privilege. 916 F.3d at 1232-34. This Court recognized that section 1806(f) leaves no room for the government to invoke the state secrets privilege in any judicial review of electronic surveillance. *Id.* at 1231-32. Section 2712(b)(4) is to the same effect.

The district court's alternative ruling that plaintiffs lack standing is equally defective. Plaintiffs have ample public evidence linking the

government's surveillance to the interception of their communications and the collection of their communication records.

Finally, plaintiffs are entitled to summary judgment on their Fourth Amendment Internet content interception claim. The government's dragnet seizures and searches of communications passing through the Internet's key domestic junctions, without a warrant and without probable cause or any showing of individualized suspicion, is unconstitutional.

STATEMENT OF JURISDICTION

The district court had jurisdiction under 28 U.S.C. § 1331.

The district court entered final judgment on plaintiffs' claims on April 25, 2019. ER 1.[1] Plaintiffs appealed on May 20, 2019. ER 82. The appeal is timely. Fed. R. App. Pro. 4(a)(1)(B).

This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF FACTS

The central dispute in this case arises under the umbrella of FISA, in which Congress asserted its authority over national security surveillance and assigned to the judiciary the crucial role of reviewing the legality of surveillance. *Fazaga* recounts FISA's well-known history.

In the early 1970s, intense public and congressional interest was directed at revelations of unchecked surveillance by the Executive. In 1975,

[1] The Excerpts of Record are cited as "ER [page number]." The Reporter's Transcript is cited as "[date] RT [page number]."

a Senate Select Committee (known as the "Church Committee" for its chairman, Senator Frank Church) investigated mass surveillance and other intelligence-gathering abuses by the executive branch. *Fazaga*, 916 F.3d at 1233. "The Church Committee documented 'a massive record of intelligence abuses over the years,' in which 'the Government ha[d] collected, and then used improperly, huge amounts of information about the private lives, political beliefs and associations of numerous Americans.' [Citation.] The Committee concluded that these abuses had 'undermined the constitutional rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability [were not] applied.'" *Id.* (quoting Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, 289, 290 (1976)); *see also In re NSA Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1115-17 (N.D. Cal. 2008).

In response, Congress enacted FISA in 1978. 50 U.S.C. §§ 1801-1885c. FISA establishes roles for all three branches of government, providing judicial and congressional oversight of national security surveillance activities by the executive branch. FISA requires that national security surveillance occur under judicial supervision and creates judicial remedies for unlawful surveillance. *Fazaga*, 916 F.3d at 1232. To implement those remedies, Congress created the procedures of section 1806(f) directing courts to use state secrets evidence to decide unlawful

surveillance claims. *Id*. FISA "thus broadly involves the courts in the regulation of electronic surveillance relating to national security." *Id*.

To insure that surveillance no longer occurs solely on the unilateral command of the Executive, Congress mandated that the statutory methods of FISA, the Wiretap Act,[2] and the Stored Communications Act[3] ("SCA") are the "exclusive means" for conducting electronic surveillance. 18 U.S.C. § 2511(2)(f).

In October 2001, in the wake of the 9/11 attacks, Congress reaffirmed its commitment to congressional control and judicial review of national security surveillance. In the USA PATRIOT Act, Congress created new causes of action for unlawful surveillance, including the collection of communications records, and extended section 1806(f)'s procedures for using secret evidence to these new claims. 18 U.S.C. § 2712.

Yet at the same time as Congress was expanding the reach of section 1806(f), the Executive secretly began a series of mass surveillance programs directed at Americans' telephone and Internet communications and communications records. It did so solely on an assertion of executive authority, without obtaining the judicial approval required by FISA. These were later dubbed the President's Surveillance Program ("PSP").

The PSP included three programs:

---

[2] 18 U.S.C. §§ 2510-2522.

[3] 18 U.S.C. §§ 2701-2712.

(1) The bulk acquisition of stored cellphone and landline phone records from major telephone companies.

(2) "Upstream" surveillance—the mass interception and searching of emails and other Internet communications as they transit the Internet "backbone" of high-capacity fiber-optic cables controlled by major Internet providers like AT&T.

(3) The bulk collection of metadata from communications transiting the Internet (e.g., "to" and "from" addresses of emails).[4]

After several years of this secret, unaccountable surveillance, an internal rebellion by national security officials led the government in July 2004 to obtain Foreign Intelligence Surveillance Court ("FISC") orders authorizing Internet metadata bulk collection. ER 192-195; ECF No. 35-1 at 4-14, 19-31; ECF No. 228, ¶34. Several years later, congressional and public outcry arising from limited media disclosures regarding the other two programs led the government to obtain FISC orders in May 2006 for phone records bulk collection and in January 2007 for Upstream mass Internet content interception and searching. ER 413-17; ER 195-209; ECF No. 228, ¶¶33, 35.

The entry of these FISC orders ended the PSP and the executive-authority justification for the surveillance, but the underlying conduct continued. The FISC orders were broad programmatic authorizations for

[4] ER 404, 432-438, 481, 517-22; ER 1213-14, ¶¶22, 29-34; ER 192-95; ER 593-615.

mass surveillance, not warrants: they were not based on probable cause or individualized suspicion of the persons whose communications and records were being seized and searched, and did not identify the persons whose communications and records were to be seized and searched.

Plaintiffs Carolyn Jewel, Erik Knutzen, Tash Hepting, Joice Walton, and the estate of the late Gregory Hicks allege that, as part of the government's mass surveillance since 2001, their Internet communications have been intercepted, copied, and searched, their phone records have been collected, and their Internet communications metadata have been collected, along with those of millions of other innocent Americans. ER 1098.

In the years since these programs were first publicly disclosed, the government has made extensive admissions about them, including in declassified FISC opinions and two reports by the Privacy and Civil Liberties Oversight Board ("PCLOB"):[5] *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (ER 393), addressing Internet content interception and searching activities, and *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (ER 152), addressing bulk collection of phone records.

[5] The PCLOB is an executive branch agency charged with reviewing anti-terrorism activities for their impact on privacy and civil liberties. 42 U.S.C. § 2000ee.

The government ended Internet metadata bulk collection after ten years, in December 2011. ECF No. 228, ¶34. It ended phone records bulk collection after fourteen years, in November 2015. ECF No. 354-1 at 147. Upstream Internet backbone surveillance continues to this day.

Further details of the government's surveillance, and of plaintiffs' evidence supporting their claims, are discussed in sections III, IV, and V below.

PROCEDURAL HISTORY

Plaintiffs filed their class action complaint 11 years ago on September 18, 2008. ER 1098. The "government defendants" or "government" are the United States, the National Security Agency, the Department of Justice, and official-capacity defendants Donald Trump, Joseph Maguire, Paul Nakasone, and William Barr. Personal-capacity defendants are Keith Alexander, Michael Hayden, George W. Bush, Richard Cheney, David Addington, Alberto Gonzales, John Ashcroft, John McConnell, John Negroponte, and Michael Mukasey.

Plaintiffs brought Fourth and First Amendment claims for equitable relief against the government defendants (Counts I, III); Fourth and First Amendment damages claims against the personal-capacity defendants (Counts II, IV); claims seeking damages and equitable relief for Wiretap Act, SCA, and FISA violations against the government and personal-capacity defendants (Counts V to XVI); and a separations-of-powers claim (Count XVII).

In 2010, the district court dismissed plaintiffs' action for lack of standing. ECF No. 57. This Court reversed, finding that plaintiffs have standing "[i]n light of detailed allegations and claims of harm linking [plaintiffs] to the intercepted telephone, internet and electronic communications." *Jewel v. NSA*, 673 F.3d 902, 905 (9th Cir. 2011).

In 2012, plaintiffs moved for partial summary judgment that sections 1806(f) and 2712(b)(4) displace the state secrets privilege; the government cross-moved to dismiss the complaint on state secrets privilege grounds and to dismiss plaintiffs' statutory claims on sovereign immunity grounds. ECF Nos. 83, 102, 112, 119, 139, 140.

In 2013, the district court held that sections 1806(f) and 2712(b)(4) displace the state secrets privilege, held that 18 U.S.C. § 2712 waives sovereign immunity for plaintiffs' Wiretap Act and SCA damages claims (Counts IX, XII, XV), and dismissed other statutory claims as to the government defendants on sovereign immunity grounds (Counts V, VI, VII, X, XIII, XVI). ER 56, *published at Jewel v. NSA*, 965 F. Supp. 2d 1090 (N.D. Cal. 2013).

In 2014, plaintiffs moved for partial summary judgment on their Fourth Amendment Internet interception claim. ECF Nos. 261, 294-3. The government cross-moved for partial summary judgment on that claim. ECF Nos. 285, 286, 299-3.

In 2015, the district court denied plaintiffs' motion, granted the government's motion on the ground that plaintiffs lacked standing and that

the state secrets privilege barred plaintiffs' claim, and entered partial judgment under Federal Rule of Civil Procedure 54(b). ER 46. On appeal, this Court found the entry of partial judgment improper and dismissed the appeal for lack of jurisdiction. *Jewel v. NSA*, 810 F.3d 622, 631 (9th Cir. 2015).

The remaining claims plaintiffs are pursuing against the government defendants are their Fourth Amendment Internet interception claims, their Wiretap Act Internet interception claims, their SCA phone records claim, and their SCA Internet metadata claims. For these claims, the district court on remand lifted the discovery stay imposed since the beginning of the case. Plaintiffs served interrogatories, requests for admission (RFAs), and document requests on the government. The district court then required plaintiffs to limit their requests to the issue of standing, and ordered the government to respond. ER 36; 5/19/17 RT 49-54, 67-74.

Independently, the district court ordered the government to marshal and present all of the evidence relevant to plaintiffs' standing, regardless of whether it fell within plaintiffs' requests. ER 36; 5/19/17 RT 49-54, 67-74.

In 2018, the government responded *ex parte* and *in camera* with a 193-page classified declaration, together with thousands of pages of classified documents. ECF Nos. 388, 389. No new facts or evidence were disclosed to plaintiffs. Plaintiffs moved for access by their counsel to the classified materials pursuant to section 1806(f) and subject to security

clearances; the district court denied plaintiffs access. ECF Nos. 393, 400, 401; ER 34.

The government's classified declaration was in narrative form and failed to respond to plaintiffs' RFAs in the "admit" or "deny" format required by Federal Rule of Civil Procedure 36. ECF Nos. 388, 389. Plaintiffs moved to compel proper responses; the district court denied the motion. ECF No. 411; ER 29.

The district court then ordered the government to move for summary judgment on standing. ER 31. The government did so, also invoking the state secrets privilege. ECF Nos. 413, 421, 438. Plaintiffs brought a cross-motion to proceed to the merits using the procedures of sections 1806(f) and 2712(b)(4). ECF Nos. 417, 430, 441.

The district court granted the government's motion and dismissed all claims against the government defendants as barred by the state secrets privilege and for lack of standing. ER 20, 21, 22 n.3, 27. It also dismissed the claims against the personal-capacity defendants, which had been stayed throughout the litigation. ER 27 n.4. The district court also issued a classified order plaintiffs have never seen. ER 2.

ISSUES

1. Do 50 U.S.C. § 1806(f) and 28 U.S.C. § 2712(b)(4) preclude any state-secrets dismissal and require the district court to adjudicate plaintiffs' claims on the merits, using state-secrets evidence reviewed under secure *ex parte*, *in camera* procedures?

2. Is there sufficient evidence in the record (including the evidence erroneously excluded by the district court) from which a reasonable factfinder could conclude that it is more probable than not that plaintiffs have suffered injuries-in-fact supporting their claims?

3. Are plaintiffs entitled to summary judgment on their Fourth Amendment Internet interception claim?

SUMMARY OF ARGUMENT

1. The district court defied this Court's decision in *Fazaga* by dismissing plaintiffs' claims on state secrets privilege grounds. *Fazaga* holds that the judicial review procedures of section 1806(f) displace the state secrets privilege in electronic surveillance cases and are mandatory and exclusive. *Fazaga*, 916 F.3d at 1230-38. Section 2712(b)(4) extended section 1806(f)'s procedures to plaintiffs' statutory claims under the Wiretap Act and the SCA. Thus, Congress has forbidden any state-secrets dismissal of plaintiffs' claims and has required that they be decided on the merits, using secure *ex parte*, *in camera* procedures to protect state secrets. *Id.*

2. The district court erred in holding alternatively that no rational factfinder could find standing based on plaintiffs' public evidence. There is

ample public evidence, including extensive government admissions, from which a rational factfinder could conclude it is more probable than not that plaintiffs' phone records were collected, that their Internet communications were intercepted and searched, and that metadata records of their Internet communications were collected. Moreover, sections 1806(f) and 2712(b)(4) require that any secret evidence favorable to plaintiffs also be considered.

3. The district court erred in denying plaintiffs summary judgment on their Fourth Amendment Internet content interception claim. The government operates a digital dragnet, seizing and searching in bulk the communications passing through the Internet's key domestic junctions, without a warrant and without probable cause or any showing of individualized suspicion.

The Fourth Amendment protects plaintiffs' Internet communications. *Carpenter*, 138 S. Ct. at 2213-14, 2221-22; *U.S. v. Cotterman*, 709 F.3d 952, 957, 964 (9th Cir. 2013) (en banc). The suspicionless, warrantless interception of plaintiffs' Internet communications is an unconstitutional seizure, and subsequent content-searching of those communications is an unconstitutional search. It is the modern equivalent of the "indiscriminate searches and seizures conducted under the authority of 'general warrants' [that] were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980).

ARGUMENT

I. Standard Of Review

This Court reviews de novo an order granting summary judgment. *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011). The district court's state-secrets dismissal is reviewed de novo. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc).

II. Section 1806(f) And Section 2712(b)(4) Preclude Any State-Secrets Dismissal

The district court erred in dismissing this lawsuit under the state secrets privilege rather than following this Court's decision in *Fazaga* and using the procedures of sections 1806(f) and 2712(b)(4) to determine the merits of plaintiffs' claims.

A. The State Secrets Privilege

The Supreme Court created the common-law evidentiary state secrets privilege in a non-electronic surveillance case, *U.S. v. Reynolds*, 345 U.S. 1 (1953). Under *Reynolds*, once information is found to be a state secret, "[t]he privileged information is excluded and the trial goes on without it." *General Dynamics Corp. v. U.S.*, 563 U.S. 478, 485 (2011). As in any case where privileged evidence is excluded, the plaintiff may use non-privileged evidence to prove the same facts to which the privileged evidence is relevant. *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). If the plaintiff lacks sufficient evidence to prove her claims once the privileged

evidence is removed, the case is dismissed, just as in any other case where a plaintiff lacks sufficient evidence. *Id.*

In *Jeppesen*, another non-electronic surveillance case, this Court extended the *Reynolds* evidentiary privilege to require dismissal in two additional circumstances: "(2) if 'the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim'; and (3) if 'privileged evidence' is 'inseparable from nonprivileged information that will be necessary to the claims or defenses' such that 'litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets.'" *Fazaga*, 916 F.3d at 1227-28 (quoting *Jeppesen*, 614 F.3d at 1083).

B. Section 1806(f) Displaces The State Secrets Privilege In Electronic Surveillance Cases

But the state secrets privilege does not apply in electronic surveillance cases, as this Court unequivocally held in *Fazaga*: "[I]n enacting FISA, Congress displaced the common law dismissal remedy created by the *Reynolds* state secrets privilege as applied to electronic surveillance within FISA's purview." *Fazaga*, 916 F.3d at 1230.

Instead of excluding state secrets evidence, as the state secrets privilege does, section 1806(f) displaces the privilege and directs courts "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" by "review[ing] in camera and ex parte the application, order, and such other materials relating to the surveillance as

may be necessary."[6] § 1806(f). Section "1806(f) requires *in camera* and *ex parte* review in the exact circumstance that could otherwise trigger dismissal of the case;" its procedures "are expressly available, as well as mandatory." *Fazaga*, 916 F.3d at 1232, 1237.

Fazaga carefully and thoroughly analyzed "the plain language, statutory structure, and legislative history" of section 1806(f), concluding they all "demonstrate that Congress intended FISA to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance." *Fazaga*, 916 F.3d at 1238.

Accordingly, in electronic surveillance cases like this one, section 1806(f)'s complete displacement of the state secrets privilege precludes any state-secrets dismissal: "Congress's intent [was] to make the *in camera* and *ex parte* procedure the *exclusive* procedure for evaluating evidence that threatens national security in the context of electronic surveillance-related determinations. That *mandatory* procedure *necessarily overrides*, on the one hand, the usual procedural rules precluding such severe compromises of the adversary process and, on the other, *the state secrets evidentiary dismissal option*." *Fazaga*, 916 F.3d at 1231-32 (italics added, citation omitted).

Moreover, section 1806(f)'s procedures, its displacement of the state secrets privilege, and its preclusion of state-secrets dismissals apply to

[6] The full texts of sections 1806(f) and 2712 are set forth in the statutory and constitutional addendum hereto.

electronic surveillance claims brought under any statutory or constitutional provision, not just claims under FISA's civil cause of action in 50 U.S.C. § 1810. *Fazaga*, 916 F.3d at 1234-38, 1251. And it applies to plaintiffs prosecuting affirmative civil claims against the government and seeking evidence to prove their case, not just to the government's defensive use of surveillance-related evidence. *Id*. at 1237-38.

"Contrary to the Government's contention, FISA's § 1806(f) procedures are to be used when an aggrieved person affirmatively challenges, in any civil case, the legality of electronic surveillance or its use in litigation, whether the challenge is under FISA itself, the Constitution, or any other law." *Fazaga*, 916 F.3d at 1238.

C. Section 2712(b)(4) Extends Section 1806(f)'s Procedures To Wiretap Act and SCA Claims

Section 2712(b)(4) goes even farther, expanding section 1806(f)'s scope from "electronic surveillance" as defined in FISA (50 U.S.C. § 1801(f)) to include interceptions of communications under the Wiretap Act and the acquisition of communications records under the SCA. For Wiretap Act and SCA claims, section 2712(b)(4) mandates that section 1806(f)'s procedures are the "exclusive means" for handling "materials governed by" section 1806(f) (i.e., materials whose "disclosure . . . would harm the national security," § 1806(f)).

Section 2712(b)(4) displaces the state secrets privilege in Wiretap Act and SCA lawsuits because, like section 1806(f), it applies "[n]otwithstanding

any other provision of law." *See Fazaga*, 916 F.3d at 1231 (holding that Congress' identical use of "notwithstanding any other law" in section 1806(f) displaces the state secrets privilege). Federal Rule of Evidence 501 also compels this result because it mandates that common-law privileges like the state secrets privilege are abrogated whenever a "federal statute" "provides otherwise."

Section 2712(b)(4)'s broad command that it, and not the state secrets privilege, is the "exclusive means" for handling materials whose disclosure would harm national security covers the use of national security evidence for any purpose, including determining the plaintiff's standing.

D. The District Court's State-Secrets Dismissal Is Contrary To Law

1. Plaintiffs' Claims May Not Be Dismissed Under The State Secrets Privilege But Must Go Forward On The Merits

Plaintiffs' constitutional and statutory Internet content and metadata interception claims fall squarely within section 1806(f) because they are "electronic surveillance" claims under 50 U.S.C. § 1801(f)(2). Plaintiffs' statutory Internet content interception claims, statutory phone records claims, and statutory Internet metadata claims all fall within section 2712(b)(4).

Accordingly, plaintiffs' claims cannot be dismissed on state-secrets grounds but instead must go forward to a decision on the merits using the procedures of sections 1806(f) and 2712(b)(4).

2. The District Court Refused To Follow Congress's Commands In Sections 1806(f) And 2712(b)(4)

Instead of applying sections 1806(f) and 2712(b)(4) as Congress commanded and as this Court directed in *Fazaga*, the district court erroneously dismissed plaintiffs' claims as barred by the *Reynolds* state secrets privilege. ER 27.

The district court's dismissal was contrary to section 1806(f)'s mandatory displacement of the state secrets privilege, its prohibition of state-secrets dismissals, and its requirement that courts determine whether the surveillance was "lawfully authorized and conducted." *See Fazaga*, 916 F.3d at 1226-27, 1230-38.

The district court's dismissal was inconsistent not only with *Fazaga* and the plain meaning of sections 1806(f) and 2712(b)(4), but with its own earlier orders, in which it held that those statutes displace the state secrets privilege and preclude its application in this lawsuit. *Jewel*, 965 F. Supp. 2d at 1103 ("[A]s a matter of law, the FISA procedural mechanism prescribed under 50 U.S.C. § 1806(f) preempts application of the state secrets privilege"), 1104 ("the *in camera* review procedure in FISA applies and preempts the determination of evidentiary preclusion under the state secrets doctrine"), 1105 (section 2712(b)(4) makes section 1806(f)'s procedures the "exclusive means" for reviewing secret evidence in Wiretap Act and SCA cases), 1106 (section 1806(f) "occup[ies] the field" and "leaves no room for application of the state secrets privilege"); ER 37-38, 43.

Rather than heed the commands of Congress in sections 1806(f) and 2712(b)(4) it had earlier acknowledged, and this Court's commands in *Fazaga*, the district court used section 1806(f) merely to review the secret evidence for the purpose of deciding whether the state secrets privilege requires dismissal. ER 26-27. Congress, however, created sections 1806(f) and 2712(b)(4) to preclude state-secrets dismissals, not to facilitate them.

The district court could point to nothing in the text of the statutes or their legislative history that permits a court using section 1806(f)'s procedures to avoid reaching the merits and instead dismiss claims under the state secrets privilege. Nor could it cite to anything in *Fazaga* supporting its state-secrets dismissal. Moreover, the district court in its order ignored entirely section 2712(b)(4) and its requirement to use the procedures of section 1806(f).

The district court sought to distinguish *Fazaga* on the ground that in *Fazaga* the state-secrets dismissal occurred before any secret evidence had been produced. From that fact alone, it concluded that *Fazaga* and section 1806(f) left open a back door permitting a state-secrets dismissal after secret evidence has been produced.

But *Fazaga's* procedural posture does not distinguish it from this case. The district court below and the *Fazaga* district court both dismissed electronic-surveillance claims on *Reynolds* state-secrets grounds without reaching the merits. That is what *Fazaga* forbids. *Fazaga*, 916 F.3d at

1230, 1234 ("§ 1806(f)'s procedures displace a dismissal remedy for the *Reynolds* state secrets privilege").

Nothing in *Fazaga* limits its analysis to state-secrets motions to dismiss or excludes state-secrets summary judgment motions from its reach. To the contrary, *Fazaga* specifically addressed what should happen on remand *after* the motion-to-dismiss stage—the district court should use section 1806(f) and decide the merits. *Fazaga*, 916 F.3d at 1251. The same rule applies here.

3. Plaintiffs Have Demonstrated They Are Aggrieved Persons

Below, the government argued that the district court could not proceed under section 1806(f) unless plaintiffs first proved they were aggrieved persons using public evidence.

The district court noted but did not adopt this argument. ER 25. It held that no matter what the evidence showed, it would refuse to decide any issue relating to plaintiffs' claims, including whether plaintiffs were aggrieved persons or had standing. ER 20-22, 25-27.

The government's aggrieved-person argument lacks merit. First, plaintiffs have presented far more than just well-pleaded allegations showing they are aggrieved. The public evidence discussed in sections III and IV below proves that plaintiffs not only have standing but are also aggrieved persons, and that alone disposes of the argument.

Second, *Fazaga* forecloses any requirement that a plaintiff who has adequately alleged surveillance claims (as the Court has already held plaintiffs have done, *Jewel*, 673 F.3d at 908-10) must further prove "aggrieved person" status before the use of section 1806(f) is triggered. The determination of whether a plaintiff is an "aggrieved person" entitled to use section 1806(f) is based on the plaintiff's well-pleaded allegations; no evidentiary showing is required. *Fazaga*, 916 F.3d at 1216, 1238-39.

Fazaga first addressed whether the plaintiffs were "aggrieved persons" in determining they stated a claim under FISA's civil cause of action, 50 U.S.C. § 1810. *Fazaga* held the plaintiffs had adequately alleged they were "aggrieved persons" under section 1801(k) of 50 U.S.C. by alleging in detail that they were subjected to surveillance. *Fazaga*, 916 F.3d at 1216.

The Court later addressed "whether FISA's § 1806(f) procedures may be used in this case," holding that "Plaintiffs must satisfy the definition of an 'aggrieved person,' *see id.* § 1801(k)." *Fazaga*, 916 F.3d at 1238. Citing its earlier conclusion that the plaintiffs had adequately alleged they were "aggrieved persons," the Court held on the basis of their allegations alone that the "Plaintiffs are properly considered 'aggrieved' for purposes of FISA." *Id.* at 1238-39.

The Court's remand order further confirms that no additional proof of aggrieved-person status beyond well-pleaded allegations is required. The Court did *not* require that the plaintiffs make any further showing or proof

that they were aggrieved persons before the district court used section 1806(f) to review secret evidence and decide their claims on the merits.

Instead, the Court instructed the district court on remand to proceed directly to using section 1806(f) and reviewing the secret evidence to determine whether the surveillance of the plaintiffs was lawful:

"In light of our conclusion regarding the reach of FISA § 1806(f), the district court should, using § 1806(f)'s *ex parte* and *in camera* procedures, review any 'materials relating to the surveillance as may be necessary,' 50 U.S.C. § 1806(f), including the evidence over which the Attorney General asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted. That determination will include . . . whether Defendants violated any of the constitutional and statutory provisions asserted by Plaintiffs . . . ." *Fazaga*, 916 F.3d at 1251.

Fazaga thus accords with this Court's holding that whether plaintiffs are aggrieved persons "is a merits determination, not a threshold standing question." *Jewel*, 673 F.3d at 907 n.4.

Fazaga's conclusion is both binding and sensible. Congress did not limit section 1806(f) only to those who have no need of it because they already have public evidence proving their surveillance claims. "[*P*]*roof* of plaintiffs' claims is not necessary at this stage." *In re NSA Telecommunications Records Litigation*, 595 F. Supp. 2d 1077, 1085 (N.D. Cal. 2009) (italics original). Instead, all that is required to use section 1806(f) are "allegations [that] 'are sufficiently definite, specific, detailed,

and nonconjectural, to enable the court to conclude that a substantial claim is presented.'" *Id*.

Finally, section 2712(b)(4), which has no aggrieved-person test, applies here in addition to section 1806(f). Section 2712(b)(4) requires *ex parte*, *in camera* review of any "materials governed by [section 1806(f)]," i.e., "materials relating to the surveillance" whose disclosure would harm national security. It thereby independently precludes any requirement that plaintiffs prove "aggrieved-person" status before using secret evidence to decide the merits. In addition, section 2712(b)(4) permits the use of secret evidence for any purpose, including proving standing and "aggrieved-person" status.

III. Plaintiffs' Evidence Of Standing Defeats Summary Judgment

A. The Legal Standard For Standing

1. This Court's Rulings Frame The Question Of Standing

"[T]hree 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.

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 Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (citations and internal quotation marks omitted).

Quantitatively, the "invasion" of plaintiffs' interests need not be substantial: "an identifiable trifle is enough for standing." *U.S. v. SCRAP*,

412 U.S. 669, 689 n.14 (1973), *cited 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 phone and Internet records. *Jewel*, 673 F.3d at 908-09, 913.

To show injury-in-fact, plaintiffs only need to show that the government has interfered with their communications and communications records. They do not need to prove that the interference violated the Constitution, the Wiretap Act, or the SCA. Standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth v. Seldin*, 422 U.S. 490, 500 (1975); *accord Jewel*, 673 F.3d at 907 n.4, 911 n.5; *Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011). This Court warned against "conflat[ing] the ultimate merits question—whether the surveillance exceeded statutory or constitutional authority—with the threshold standing determination." *Jewel*, 673 F.3d at 911 n.5.

Likewise, it is law of the case that whether plaintiffs are "aggrieved persons" "is a merits determination, not a threshold standing question." *Jewel*, 673 F.3d at 907 n.4. The district court erroneously conflated the aggrieved-person question with the question of standing, treating them interchangeably. ER 25.

2. Plaintiffs' Burden In Opposing Summary Judgment

As the nonmoving party, plaintiffs' burden in defeating summary judgment on standing is light. Plaintiffs need only produce sufficient

evidence from which a rational factfinder could conclude it is more likely than not—and not any greater degree of certainty—that, over the many years of the government's surveillance, at least one of each plaintiff's Internet communications was intercepted, copied, or redirected, and that at least one of their phone records and Internet metadata records was collected. *See Bravo*, 665 F.3d at 1083; *Lujan*, 504 U.S. at 561; *Anderson v. Liberty Lobby*, 477 U.S. 242, 252 (1986).

The Court views the evidence and draws all inferences in the light most favorable to plaintiffs, the nonmoving party. *Bravo*, 665 F.3d at 1083. The evidence must be considered "as a whole;" no single piece of evidence need carry the entire weight of showing plaintiffs' injuries. *Pavoni v. Chrysler Group*, 789 F.3d 1095, 1098 (9th Cir. 2015).

"As in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence." *U.S. Postal Serv. Bd. of Governors v. Aikens*, 460 U.S. 711, 714 n.3 (1983).

This Court reviews the district court's exclusion of evidence for abuse of discretion. *Las Vegas Sands, LLC v. Nehme*, 632 F.3d 526, 532 (9th Cir. 2011).

B. Plaintiffs Have Standing For Their Phone Records Claims

1. The Public Evidence

The public evidence establishes injury-in-fact by demonstrating 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 records.

1. The government admits that major phone companies participated in the program, and that all of the many millions of Americans who were their customers had their phone records collected:

- The FISC describes the phone records program as the "production *by major telephone service providers* of call detail records for *all* domestic, United States-to-foreign, and foreign-to-United States calls." ER 666 (italics added).
- The PCLOB states: "[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 . . . ." ER 177.
- "[M]illions of telephone numbers [were] covered," and for each, "the agency obtains a record of all incoming and outgoing calls." ER 270.

2. The phone records program included plaintiffs' phone providers AT&T and Verizon Wireless:

- The government disclosed AT&T, Verizon, and Verizon Wireless's participation in the phone records program in a *New York Times* FOIA lawsuit. To settle the litigation, the government disclosed a letter from the NSA to the FISC (the "NSA Letter") naming them as telephone companies that

produced phone records in bulk as required by a FISC order. The *New York Times* subsequently published the NSA Letter.[7] ER 869; ER 845-46, ¶¶3, 4; ER 848-907; ER 147-48, ¶¶2-3, 5-6; *New York Times v. NSA*, No. 15-cv-2383 (S.D.N.Y. Mar. 31, 2015), Complaint (ECF No. 1), ¶9; *id*., Scheduling Order (ECF No. 10).

- During the 2001-2015 period the government collected phone records in bulk, all plaintiffs were phone customers of AT&T. Plaintiffs Hepting and Walton were also Verizon Wireless customers. ER 1002-03, ¶¶22-23; ER 1004; ER 1009, ¶¶18-20; ER 1011; ER 1013, ¶¶4-5; ER 1017, ¶¶20-22; ER 1018; ER 1022, ¶¶20-24; ER 1024.

3. The NSA Letter alone proves plaintiffs' standing. Additional supporting evidence confirms AT&T's and Verizon's participation:

- During the period the bulk phone records program was operating under FISC orders, both AT&T and Verizon admitted they provided "non-content" information, which includes phone

[7] Exhibit A of ECF No. 417-4 is a FISC "primary order" compelling the bulk production of phone records from multiple phone companies. It was issued in FISC docket BR 10-10 ("BR" for "Business Records"). ER 849-67. Exhibit B is an NSA Inspector General Report excerpt that includes the NSA Letter to the FISC. ER 869-907. The letter's caption identifies AT&T, Verizon, Verizon Wireless, and Sprint as companies compelled by primary order BR 10-10 to produce their phone records. ER 896-97 (Ex. B, pp. 28-29).

records, about their customers' communications to the government pursuant to FISC orders. ER 911, 928.

- An NSA Office of Inspector General draft report ("the NSA Draft OIG Report") describes how "Company A" and "Company B" provided phone records and Internet metadata and participated in the interception of Internet content. ER 121-22, 128-29. The report explains that Company A and Company B were the two largest providers of international telephone calls to and from the United States, and other evidence shows that the two largest international call providers were AT&T and MCI/Worldcom (which later merged with Verizon). ER 121; ER 1030.
- The government released a FISC order requiring Verizon Business Network Services ("VBNS") to produce phone records. ECF No. 144, Ex. A at 1, 4; *In re FBI*, No. BR 13-80, 2013 WL 5460137 (Foreign Intel. Surv. Ct. Apr. 25, 2013) (primary order in BR 13-80). It supports the inference that other Verizon business units, including Verizon Wireless, were also subject to phone records orders, since it makes little sense that the government would have compelled only one unit of the company to participate, especially given the admitted size of the program.

> Moreover, VBNS's phone records also include records of all calls of *non*-VBNS customers like plaintiffs that are calls to or from any VBNS customer. ER 939, 941 (George Molczan, *A Legal And Law Enforcement Guide To Telephony*, pp. 34, 38 (2005)).[8] So the VBNS records the government admits acquiring would contain records of calls between plaintiffs and VBNS customers.

The evidence above is more than sufficient to demonstrate standing. Drawing all inferences in plaintiffs' favor and viewing the evidence as a whole, a rational factfinder could easily conclude that, more probably than not, at least one phone record of each plaintiff was collected.

2. The Size And Method Of The Phone Records Program Is Additional Evidence Of Plaintiffs' Standing

Additionally, the government's admissions about the size and method of the phone records program confirm that it could not have operated without the participation of AT&T, the largest phone company, and Verizon.

[8] The fact that a phone call between customers of two different phone companies generates two phone records—one held by each phone company—is not subject to reasonable dispute. The district court did not rule on plaintiffs' request to take judicial notice of this fact, which "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned," i.e., the Molczan treatise. Fed. R. Evid. 201(b)(2); ECF No. 429-3 at 6 n.3. Plaintiffs request that this Court take judicial notice.

The method 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, 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). ER 184-86, 270, 298. The third hop can result in looking at the phone records of hundreds of thousands of persons. ER 184.

The PCLOB estimated that the three-hop searches conducted by the NSA in 2012 alone yielded the phone records of 120 million persons. ER 185-86. Three-hop contact-chaining on that scale required the government to collect the phone records of hundreds of millions of persons. A phone records program that excluded AT&T (with 163 million customer phone lines) and Verizon (with 128 million customer phone lines) could not perform three-hop contact chaining reliably—contact-chaining would hit a wall whenever it led to an AT&T or Verizon number.[9] A program that

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

Verizon Communications Inc.'s SEC Form 10-Q, at 39, 42 (July 31, 2018), *available at* https://www.sec.gov/Archives/edgar/data/732712/000073271218000044/a2018q210-q.htm.

(footnote continued on following page)

excluded AT&T and Verizon certainly could not perform three-hop searches yielding the phone records of 120 million persons. No other conclusion is mathematically possible, for there is no other phone company in America with anywhere near 120 million customers. *See* ER 666 (phone records program involved "major telephone service providers"). This conclusion is an evidence-based deduction, not speculation. It further supports plaintiffs' standing.

Citing *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015), the district court rejected this conclusion as too speculative. It made three errors.

First, it treated this deduction as though it had to bear the entire weight of proving plaintiffs' phone-records standing. It does not; it is only one thread in the fabric of evidence.

Second, plaintiffs' evidence is much broader and more robust than the evidence in *Klayman*. The *Klayman* plaintiffs did not submit the FISC and PCLOB disclosures cited above. They did not submit the NSA Letter or the NSA Draft OIG Report, both of which provide direct evidence of AT&T's and Verizon's involvement. They also did not submit evidence of the size of AT&T's and Verizon's subscriber bases. *Klayman* thus did not consider whether exclusion of AT&T and Verizon from the program would have left

---

(footnote continued from previous page)
The district court did not rule on plaintiffs' request for judicial notice of these two documents. ECF No. 429-3 at 6 nn.1, 2. Plaintiffs request that this Court judicially notice them.

the government still able to perform three-hop searches yielding the phone records of 120 million persons.

Third, the district court ignored that *Klayman* reviewed a preliminary injunction, applying the higher, substantial-likelihood standard of proof, not the lower more-likely-than-not standard that applies here. 800 F.3d at 564, 568.

3. The District Court Abused Its Discretion In Excluding The NSA Letter And The NSA Draft OIG Report

a. The NSA Letter

The district court excluded on state secrets privilege and authentication grounds the NSA Letter the government disclosed to the *New York Times*. ER 18-19. That was an abuse of discretion because it applied incorrect legal standards. *Las Vegas Sands*, 632 F.3d at 532.

The state secrets privilege objection fails, first, because section 2712(b)(4) displaces the state secrets privilege for plaintiffs' phone records SCA claims.

Second, even if the privilege were not displaced, it still would not apply because the NSA Letter is public, not secret. It was published by the *New York Times*. A "claim of privilege does not extend to public documents." *Jeppesen*, 614 F.3d at 1090. To call the NSA Letter "secret" is an Orwellian abuse of the English language.

The district court improperly relied on *Al-Haramain Islamic Foundation v. Bush*, 507 F.3d 1190 (9th Cir. 2007), in excluding the NSA Letter. Unlike the NSA Letter, however, the secret document in *Al-Haramain* "remains secret." *Id*. at 1202. The *Al-Haramain* document was never publicly disclosed, much less published by the *New York Times*.

The district court also applied an incorrect legal standard in excluding the NSA Letter for lack of authentication, erroneously ruling that the NSA Letter could only be authenticated by a government acknowledgment. Authentication, however, "does not erect a particularly high hurdle." *U.S. v. Dhinsa*, 243 F.3d 635, 658 (2d Cir. 2001) (citation omitted). All that is required is "evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). Authentication certainly does not require an admission by a party-opponent.

In any event, the government made a judicial admission of authenticity when it produced the NSA Letter in FOIA litigation in response to a request for only NSA Inspector General reports. *Orr v. Bank of America*, 285 F.3d 764, 777 n.20 (9th Cir. 2002).

The declaration of *New York Times* counsel David McCraw further authenticates the NSA Letter. First, it confirms the government produced the NSA Letter, verifying the government's judicial admission. ER 147-48, ¶¶5-6. Second, the declaration shows the NSA Letter "is from the office where items of this kind are kept" (Fed. R. Evid. 901(b)(7)(B)) by showing the FOIA litigation was against the NSA, requested only NSA documents,

and the NSA was the entity that produced the NSA Letter. ER 147-48, ¶¶2-6.

Additionally, the authenticity of the NSA Inspector General's Report of which the NSA Letter is a part is undisputed. "The appearance, contents, substance, internal patterns, or other distinctive characteristics of the" NSA Letter, "taken together with all the circumstances" of its production by the government as part of an authentic NSA Inspector General's Report, is sufficient to authenticate the NSA Letter. Fed. R. Evid. 901(b)(4); *Orr*, 285 F.3d at 778 n.24.

b. The NSA Draft OIG Report

The district court similarly abused its discretion in excluding the NSA Draft OIG Report on states secrets privilege grounds and for lack of authentication. Section 2712(b)(4) displaces the state secrets privilege. Additionally, as with the NSA Letter, the NSA Draft OIG Report is not secret but has been published by the *Guardian*, and thus is outside the state secrets privilege. ECF No. 147 at 2; *Jeppesen*, 614 F.3d at 1090.

The NSA Draft OIG Report is a record or statement by a government agency, and Edward Snowden's testimony authenticates it by showing it "is from the office where items of this kind are kept," i.e., from the files of the NSA. ER 88; Fed. R. Evid. 101(b)(4); 901(b)(7)(B); *U.S. v. Estrada-Eliverio*, 583 F.3d 669, 673 (9th Cir. 2009) (Rule 901(b)(7)(B) requires "only personal knowledge that a document was part of an official file"). The district court asserted Snowden's authentication was "not persuasive, either

by way of his current declaration or in the future through live testimony," but offered no supporting reasoning. ER 19.

Independently, "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the [NSA Draft OIG Report], taken together with all the circumstances" are alone "sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a), (b)(4) ; *Orr*, 285 F.3d at 778 n.24. The government did not even attempt to argue that the NSA Draft OIG Report is not what it appears to be, and presumably has confirmed its authenticity in its classified responses to Plaintiffs' RFA Nos. 50-52. ECF 379-1, Ex. C at 56.

C. Plaintiffs Have Standing For Their Upstream Internet Interception Claims

The public evidence demonstrates it is more likely than not that 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 Upstream Internet interception claims.

The government's admissions dovetail with plaintiffs' eyewitness and expert evidence. They show that in Upstream surveillance the government intercepts communications in transit over the junctions connecting the Internet backbones of different communications providers, including AT&T; that the entire stream of communications flowing through these junctions is

copied, including plaintiffs' communications; and that the copies are then filtered and searched by the government.

1. Government Admissions

The government admits:

Upstream collects communications as they are in transit on the Internet backbone—high-capacity circuits operated by major Internet providers: "[T]he [NSA] intercepts communications directly from the Internet 'backbone'" using "NSA-designed upstream Internet collection devices [that] acquire transactions[10] as they cross the Internet." ER 521, 436; *see also* ER 404, 432-38, 481.[11]

The interceptions occur at the point where the Internet backbone circuits of different Internet providers connect, "in the flow of communications between communications service providers." ER 432. Other evidence explains that these junctions between the backbone circuits of different providers are called "peering links." ER 991, ¶48(e); ER 970-71, ¶¶34-36.

---

[10] The NSA defines a "transaction" as a single communication or a group of communications traversing the Internet; a transaction may be "broken up into a number of data packets that take different routes to their common destination." ER 436, 522 & n.517.

[11] *See also* ECF No. 253-3, Ex. B at 3 ("NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States"); ER 715 n.3; ER 822 ("the acquisition of Internet communications as they transit the 'internet backbone' facilities").

The government "filters" the mammoth communications streams flowing through the peering links in an imperfect attempt to exclude purely domestic communications. ER 434-35, 438.

The government then searches the remaining communications from top to bottom for what the government calls "selectors." *See* ER 404, 430 433-34, 438. The government says the selectors it searches for are communications identifiers such as email addresses and phone numbers. ER 429, 434.

The NSA's interceptions occur "with the compelled assistance of providers that control the telecommunications 'backbone' over which . . . Internet communications transit." ER 404.

"[S]electors 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 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."[12] ER 433-34.

The NSA Draft OIG Report, discussed above, shows AT&T's participation in Upstream Internet content surveillance. ER 108, 128; ER 1040; ER 402.

[12] "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.

2. Evidence From AT&T, Its Employees, Plaintiffs, and Plaintiffs' Experts

AT&T is a major provider of Internet services and one of the largest Internet backbone network operators. ER 1064, ¶122; ER 986, ¶26; ER 970-71, ¶36.

AT&T admits it provides communications content to the government pursuant to FISC orders. ER 911.

AT&T's documents and the testimony of AT&T employees Mark Klein, James Russell, and Philip Long provide direct evidence of AT&T's involvement in Upstream surveillance. Plaintiffs' experts Scott Marcus, Dr. Brian Reid, Professor Matthew Blaze, and Ashkan Soltani provide further testimony supporting standing. This evidence is summarized below and discussed in detail in the Upstream Evidentiary Discussion in section V.

All of the communications flowing across fiber-optic cables of the peering links connecting AT&T's Internet backbone network at its Folsom Street Facility in San Francisco with the Internet backbones of other Internet providers were copied using optical "splitters." ER 1212-15, ¶¶19, 21-34, 36; ER 1216-1339; ER 1197-98, ¶6; ER 1200-04, ¶¶10-12, 15, 19-23; ER 957-58, ¶¶11-20; ER 1047-52, ¶¶56-58, 62, 70-73, 77; ER 1060-63, ¶¶109, 113-18; ER 970-71, ¶¶34-37. Without any commercial or engineering purpose, AT&T rerouted Internet backbone traffic in California to flow through the Folsom Street Facility. ER 956-59, ¶¶7-20, 25.

After copying all of the communications on the peering links, the splitters then redirect the entire stream of copied communications to a secure NSA-controlled room at the Folsom Street Facility—the "SG3" room. ER 1212-15, ¶¶19, 24-34, 36; ER 1220, 1241, 1245, 1250, 1255, 1280, 1284, 1293-94, 1322-23, 1326-27; ER 958, ¶¶21-22.

The SG3 room contains spy equipment capable of filtering and searching the copied communications. ER 1214-15, ¶35, ER 1284; ER 1197-98, ¶6; ER 1201-04 ¶¶15, 19, 22-23. The SG3 room contains a "Data Filter Cabinet." ER 1284. It also contains a Narus Sematic Traffic Analyzer capable of searching the contents of communications. *Id*.; ER 1053-55, ¶¶79-85.

Importantly, the government *admits* plaintiffs' evidence shows that the splitters copy all the traffic passing over AT&T's peering links and that at least one of each plaintiff's communications has passed over those peering links and been copied and diverted to the SG3 room. ECF 421 at 13:2-13.

Plaintiffs' experts confirm that plaintiffs' Internet communications have passed through the peering links, have been copied by the splitters, and have been diverted to the SG3 room. ER 982, ¶11; ER 989-90, ¶¶39-44; ER 961, ¶2; ER 965-66, ¶¶21-22; ER 973-74, ¶¶48-51; ER 975, ¶56; ER 1058-61, ¶¶98-109; *see* ER 994, ¶2; ER 996-98, ¶¶16-18, 21-25.

The experts also confirm that the splitters copy all communications on the peering links and confirm the surveillance capabilities of the spy equipment in the SG3 room. ER 1045-47, ¶¶44-49, 56; ER 1049-61, ¶¶62,

68-89, 94-109; ER 961, ¶2; ER 964-66 ¶¶20, 22; ER 971-74, ¶¶37-45, 47-51; ER 988, ¶34.

AT&T employee Klein operated the splitters that diverted the copied communications to the SG3 room. ER 1212-15, ¶¶19-36. Klein and fellow employee Long were excluded from the SG3 room because only personnel cleared by the NSA were permitted inside. ER 1211-12, ¶¶14, 17-18; ER 958, ¶21. Klein observed NSA agents meeting with his co-workers who were in charge of the SG3 room. ER 1211-12, ¶¶10, 12, 14, 16. In the course of his employment, AT&T management informed him in advance of these NSA meetings and discussed the results with him afterwards. ER 1210-12, ¶¶8-10, 16.

AT&T installed similar splitters in other cities, including Seattle, San Jose, Los Angeles, San Diego, and Atlanta. ER 1215, ¶36; ER 1233; *see* ER 1062-63, ¶¶113-18.

The government's admissions that communications are intercepted directly from the Internet backbone by devices sitting on the backbone and then searched corroborate the process described in the AT&T documents and the AT&T employees' testimony. ER 433-34, 436, 521; ER 990-91, ¶¶47-51. The government's admission that it places its surveillance devices in the peering links carrying "the flow of communications between communication service providers" describes the splitters, and the SG3 room spy equipment is capable of performing the subsequent filtering and

searching the government admits to. ER 432; ER 990-91, ¶¶47-51; ER 970-71, ¶¶34-36; ER 1284.

3. The Evidence Establishes Injury-In-Fact

This evidence is certainly sufficient to prove injury-in-fact, i.e., that the Internet communications of plaintiffs were more likely than not copied and diverted by Upstream surveillance. *See* ER 982, ¶11; ER 989-90, ¶¶39-44; ER 961, ¶2; ER 965-66, ¶¶21-22; ER 973-75, ¶¶48-51, 56; ER 1047, ¶56; ER 1050-51, ¶¶68-73; ER 1060-61, ¶¶108-09. Drawing all inferences in plaintiffs' favor and viewing the evidence holistically, 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. Indeed, the government admits that plaintiffs' evidence is sufficient to show this. ECF No. 421 at 13:2-13.

The initial copying and redirection of plaintiffs' communications by the splitter is sufficient for standing—it is far more than an identifiable trifle. Whatever further processing or searching occurs *after* the bulk copying by the splitters and redirection to the SG3 room does not affect plaintiffs' standing.[13] Standing also does not require that the government permanently retain plaintiffs' communications.

[13] In its secret filings, the government might be contending that AT&T's surveillance devices were solely for gathering "to" and "from" email addresses for the government, not for selector searching. Even if that were so, the initial copying and redirection of the entire communication would still give plaintiffs standing for their Fourth Amendment and Wiretap Act

(footnote continued on following page)

The district court was wrong in suggesting that plaintiffs, in addition to showing the fact of interception, also needed to show as well the government's purposes and the means by which it accomplishes it searches. ER 16. In doing so, it erroneously strayed far from "the threshold standing determination" into the merits. *Jewel*, 673 F.3d at 911 n.5. In any event, the PCLOB tells us exactly what happens to communications transiting peering links like those captured and copied by the splitter and sent to the SG3 room—they are filtered and searched for "selectors."

4. The Copying And Diversion Of Plaintiffs' Communications Is Fairly Traceable To The Government

Admitting the sufficiency of plaintiffs' evidence showing that their communications are copied by the splitters and diverted to the SG3 room, the government disputes only whether AT&T's surveillance system has any connection to the government's acknowledged Upstream surveillance. ECF No. 421 at 12:20-23.

The question of the government's connection to the injury of the initial copying and redirection of plaintiffs' communications is a question of traceability, not injury-in-fact.

(footnote continued from previous page)
Internet interception claims. This is because the "to" and "from" addresses of an email reside inside its contents, so to collect the addresses it is necessary to copy and examine the contents of the email. ER 982, ¶12; ER 984-89, ¶¶22, 27, 33, 38; ER 965-66, ¶22(c); ER 976, ¶¶59-61.

As the Court previously found, "the harms Jewel alleges—invasion of privacy and violation of statutory protections—can be directly linked to this acknowledged surveillance program." *Jewel*, 673 F.3d at 912. There is plenty of evidence from which a rational factfinder could conclude that AT&T's copying and diversion of plaintiffs' communications is, more probably than not, "fairly traceable" to the government. *Id*. at 908.

This evidence—discussed above and in detail in the Upstream Evidentiary Discussion in section V—includes:

- Klein's testimony showing the NSA's connection to the Folsom Street Facility and to the equipment and activities present there, including the splitters, the Data Filter Cabinet, and the Narus content-searching equipment;
- the government's admissions concerning Upstream surveillance that match Klein's evidence, including that it is directed at peering links operated by telecommunications providers and that it operates by filtering and searching communications passing over the peering links;
- AT&T's admission that it performs FISA content surveillance;
- the NSA Draft OIG Report showing AT&T participates in Upstream;
- Long's testimony that Internet backbone traffic was funneled to the Folsom Street Facility for no commercial or engineering purpose and that he was denied access to the SG3 room;

- Russell's testimony confirming the presence of filtering and searching spy equipment in the SG3 room; and
- expert Marcus's testimony that there is no commercial reason for AT&T's copying and diversion of communications and that government surveillance is the most probable explanation.

5. The District Court Erroneously Excluded Internet Interception Evidence

In attempting to buttress its conclusion that plaintiffs lack standing for their Internet interception claims, the district court erroneously excluded much of plaintiffs' evidence. (The details of plaintiffs' evidence are set forth in the Upstream Evidentiary Discussion in section V.)

a. Russell's direct evidence of the spy equipment in the SG3 room and the Internet room is admissible.

AT&T's Managing Director-Asset Protection James Russell (1) confirmed the authenticity of the three AT&T documents ("the AT&T documents," ER 1216-1339) attached to Klein's declaration as Exhibits A, B, and C, and (2) independently testified to the matters stated in the AT&T documents and in Klein's and Marcus's declarations. ER 1197-98, ¶6; ER 1200-04, ¶¶10-12, 15, 19-23.

Russell did so in support of AT&T's unsuccessful attempt in the related *Hepting v. AT&T* litigation to exclude on trade secret grounds the AT&T documents and statements made by Klein and Marcus. *Hepting v. AT&T*, No. 06-cv-0672 (N.D. Cal.), ECF No. 220. AT&T admitted that the

AT&T documents are authentic. *Hepting v. AT&T*, ECF No. 228 at 1:2 (Klein exhibits "belong[] to AT&T").

The district court erred in excluding Russell's testimony as "unreliable." ER 16. The district court erroneously believed that Russell's knowledge of the Folsom Street Facility was derived solely from Klein's declaration and the AT&T documents. *Id*.

But Russell testified from his "personal knowledge of the facts" based upon his role at AT&T that the equipment and operations at the Folsom Street Facility described by Klein and by the AT&T documents actually are present there. ER 1197, ¶1. This includes the spy equipment in the SG3 room listed in Exhibit C and the splitter equipment in the Internet room. ER 1284; ER 1197-98, ¶6; ER 1201-04, ¶¶15, 19-23. He does not rely on Klein or the AT&T documents for the veracity of anything they state but instead attests that the facts they state are true from his personal knowledge. ER 1197, ¶1. The entire point of Russell's testimony on AT&T's behalf was that because the facts concerning the Folsom Street Facility stated in the Klein and Marcus declarations and in the AT&T documents were true, AT&T believed it would be harmed by their public disclosure.

b. The AT&T documents are admissible.

The district court abused its discretion in excluding the three AT&T documents attached to Klein's declaration (ER 1216-1339) as hearsay not subject to the business records exception. ER 16. The documents are admissible on multiple grounds.

First, the AT&T documents are admissible business records under Federal Rule of Evidence 803(6). The district court's assertion that they did not satisfy Rule 803(6)(A)'s contemporaneity requirement is demonstrably wrong. ER 16. The AT&T documents satisfy Rule 803(6)(A)'s requirement that business records be created "at or near the time" because they were created within a few weeks of the events and conditions they describe. Fed. R. Evid. 803(6); *Selig v. U.S.*, 740 F.2d 572, 578 (7th Cir. 1984) (six-month gap between event and record satisfied Rule 803(6)).

The documents are dated January 13, 2003 (Exhibit A); January 24, 2003 (Exhibit B), and December 10, 2002 (Exhibit C). ER 1217, 1261, 1282. Klein observed the SG3 room nearing completion in January 2003. ER 1211, ¶¶11-12, 14. Exhibit B shows that the connections of the peering links to the splitters were completed between January 22, 2003 and February 27, 2003. ER 1280.

Moreover, Klein relied on the AT&T documents to do his job connecting peering links to the splitters and the splitters to the SG3 room. ER 1212-15, ¶¶19, 22, 25-31, 34, 36. If the AT&T documents had not been accurate and trustworthy, AT&T's Internet backbone operations at the Folsom Street Facility would have been disrupted.

Second, the AT&T documents are admissible under Federal Rule of Evidence 803(3) even if, as the government argued (ECF No. 421 at 16), they are considered to be only statements of future plan or intent for using

splitters to intercept the peering links and send the copied communications to the SG3 room for analysis by the spy devices there.

Importantly, they are also admissible to show that AT&T thereafter installed the spy devices in the SG3 room and used the splitters to intercept the peering links in accordance with the documents. *U.S. v. Best*, 219 F.3d 192, 198 (2d Cir. 2000) (statement of plan or intent can be used to "prove that the declarant thereafter acted in accordance with the stated intent"); *U.S. v. Donley*, 878 F.2d 735, 737-38 (3d Cir. 1989) (same); *U.S. v. Astorga-Torres*, 682 F.2d 1331, 1335-36 (9th Cir. 1982) (same).

Third, the AT&T documents are admissible nonhearsay under Federal Rule of Evidence 801(d)(2)(D) as statements by AT&T as the government's agent. The PCLOB makes clear that telecommunications providers like AT&T conduct Internet backbone surveillance as agents of the government because they act on the government's behalf and subject to its control. ER 404, 432-36; *U.S. v. Bonds*, 608 F.3d 495, 506 (9th Cir. 2010).

AT&T admits it conducts FISA surveillance for the government. ER 911. The evidence discussed in the next section shows the NSA's connection to the Folsom Street Facility and its surveillance devices, and the NSA's control of AT&T's surveillance operations. The NSA Draft OIG Report also shows that AT&T conducts Upstream surveillance on behalf of the government and subject to its control.

The AT&T documents thus concern matters within the scope of AT&T's assistance to the government in conducting surveillance and were

made during the existence of that relationship. Fed. R. Evid. 801(d)(2)(D). The government's classified responses to Plaintiffs' RFAs Nos. 53-61—if not evasive—should also establish that the AT&T documents evidence AT&T's participation in the government's Internet backbone surveillance. ECF 379-1, Ex. C at 56-57.

Finally, because Russell independently testifies to the truth of the information in the AT&T documents, even if the documents themselves were not admissible, all of the relevant facts within them would be in the record through Russell's testimony.

c. Klein's evidence of the NSA's connection to the splitters and the SG3 room is admissible.

The district court's exclusion of Klein's testimony regarding the NSA's connection to the Folsom Street Facility's surveillance devices for lack of personal knowledge was an abuse of discretion.

Klein's testimony of the NSA's involvement with the splitters and SG3 room at his workplace is admissible because it is based on his personal observations and experiences on the job. "[P]ersonal knowledge and competence to testify are reasonably inferred from [employees'] positions and the nature of their participation in the matters to which they swore." *Barthelemy v. Air Lines Pilots Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990). It is no different than any other testimony by an employee regarding her on-the-job experiences, her observations of co-workers, her company's policies and practices, or its interactions with another entity. *Great American Assur.*

Co. v. Liberty Surplus Ins. Corp., 669 F. Supp. 2d 1084, 1089 (N.D. Cal. 2009) (employee may testify to company policies based on her "experience and perceptions" on the job); *Sjoblom v. Charter Comms.*, 571 F. Supp. 2d 961, 968-69 (W.D. Wis. 2008) (employees may testify about supervisors' and co-workers' activities they observe).

Employees may testify about the functions and activities of others within the organization that employs them and about the relationship between the organization and outside entities, including government entities; such testimony is not inadmissible hearsay because it is based on personal, on-the-job observations. *U.S. v. Neal*, 36 F.3d 1190, 1206 (1st Cir. 1994).[14] And an employee's "[p]ersonal knowledge can include 'inferences and opinions, so long as they are grounded in personal observation and

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

experience.'" *Neal*, 36 F.3d at 1206; *see also* Fed. R. Evid. 701 (lay opinion admissible).

Thus, Klein is competent to testify about his personal knowledge and observations on the job regarding AT&T's relationship with the NSA:

- Klein, who otherwise had keys and free access to all parts of AT&T's Folsom Street Facility, has personal knowledge that the reason he was excluded only from the SG3 room is because AT&T's policy was to restrict access to only persons cleared by the NSA, even in emergencies. ER 1212, ¶¶17, 18. Long confirms that AT&T restricted access to the SG3 room, contrary to normal practices. ER 958, ¶21.
- Klein testified from personal knowledge about visiting the SG3 room under construction, where he saw "FSS #2," whom Klein had observed meeting with an NSA agent and whom Klein knew to be in charge of the room, installing equipment. ER 1211-12, ¶¶10, 12, 14, 17.
- Klein's statements that "The NSA agent came and met with FSS #2" and "The NSA agent did come and speak to FSS #1" are direct personal observations, not hearsay. ER 1211-12, ¶¶10, 16.

In addition to these personal observations of the NSA's involvement, the statements made to Klein by AT&T's management and his co-workers

about the NSA's activities and NSA's connection to the SG3 room are also admissible. ER 1211-12, ¶¶10, 16.

They are admissible under *Neal* as knowledge learned by Klein on the job, just as the witness in *Neal* testified about her employer's relationship with a federal agency (the Federal Deposit Insurance Corporation) and the states where its customers were located based solely on information she learned from hearsay statements in documents she reviewed. 36 F.3d at 1206.

The statements made to Klein are also admissible nonhearsay under Rule 801(d)(2)(D) because, as discussed above, AT&T is the government's agent in assisting in electronic surveillance. AT&T's role as agent is shown by AT&T's admission that it conducts FISA surveillance, by Klein's observations of the visits by NSA agents and the exclusion of uncleared persons from the SG3 room, by the statements themselves, and by the NSA Draft OIG Report. *Id*.

The AT&T management email and the statements by Klein's manager regarding upcoming NSA visits (ER 1211-12, ¶¶10, 14, 16) are independently admissible under Federal Rule of Evidence 803(3) as statements of future intention. They state AT&T's intention to meet with the NSA, that the intended purpose of the first meeting was for "the NSA agent . . . to interview FSS #2 for a special job" managing the SG3 room, that the intended purpose of the second meeting was to discuss "FSS #3's suitability to perform the special job that FSS #2 had been doing," and that AT&T's

plan and intent was to cooperate with the NSA. Further, they are also evidence that AT&T employees actually met with NSA agents and managed the SG3 room to facilitate the NSA's purposes, and that AT&T did cooperate with the NSA. *Best*, 219 F.3d at 198; *Donley*, 878 F.2d at 737-38; *Astorga-Torres*, 682 F.2d at 1335-36.

d. Klein has personal knowledge of what data was copied by the splitters and sent to the SG3 room.

The district court erred in excluding for lack of personal knowledge Klein's testimony regarding "what data were actually processed . . . in the [SG3] room." ER 16. Klein knew what data were processed in the SG3 room because he controlled the data that went into the SG3 room. That was his job. Klein operated the splitters that copied the data from the peering links and sent it to the SG3 room, and he describes in detail the circuits connected to the splitters and the data they carry. ER 1211, ¶15; ER 1213-15, ¶¶22, 25-36.

e. The district court abused its discretion in excluding the expert evidence.

The district court abused its discretion in excluding the expert evidence of Marcus, Dr. Reid, and Professor Blaze analyzing the splitter's copying and diversion of communications transiting the peering links. ER 16-17. It contended the experts based their analysis on "[Klein's] hearsay and speculation," ignoring that, as discussed above, Klein has personal knowledge that the splitters he operated copied and sent to the SG3

room all the communications transiting the peering links, and thus his testimony on those subjects is admissible.

Notably, the government never presented any expert testimony challenging plaintiffs' experts; instead, it conceded that plaintiffs' evidence showed their communications had been copied by the splitters and diverted to the SG3 room. ECF No. 421 at 13:2-13.

Russell's testimony provides an independent and sufficient basis for Marcus's analysis of the spy equipment in the SG3 room, as well as the experts' analysis of the splitters. Marcus was also entitled to rely on the AT&T documents evidencing the equipment in the SG3 room, which the district court erroneously excluded.

The district court also erroneously excluded Soltani's explanation showing how, even apart from AT&T's surveillance architecture, users of Gmail and Yahoo mail like plaintiffs were likely caught up in Upstream surveillance. ER 994, ¶2; ER 996-98, ¶¶16-18, 21-25. It asserted Soltani's opinions were "not based on sufficient facts or data" but identified nothing that was lacking or suspect in their foundation. ER 17. Soltani's opinions rest on his unchallenged knowledge of Internet operations of Gmail and AT&T email and his expertise in Internet operations, including serving as the FTC's Chief Technologist.

D. Plaintiffs Have Standing For Their Internet Metadata Claims

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

The government admits:

- The Internet metadata program used devices to collect metadata from Internet communications during their transmission over the Internet. ER 616-21, 667. It included collecting metadata for "all email . . . traversing any of the communications facilities at the specified locations" ER 673.
- Like the phone records program, it was a broad-based and "massive" collection program. ER 707. 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, contact-chaining required "the collection of both a huge volume and a high percentage of unrelated communications." ER 601.
- Over time, the Internet metadata program expanded "to acquire a much larger volume of metadata at a greatly expanded range of facilities." ER 663. It was no longer limited to "streams of data with a relatively high concentration of Foreign Power

communications" but was "sweeping" and "wholly non-targeted bulk production." ER 666; ER 673. This "11- to 24-fold increase in volume" correspondingly resulted in "captur[ing] metadata for a larger volume of U.S. person communications." ER 664, 667 n.61.

- The FISC found that throughout the program's existence the government systemically overcollected Internet metadata far beyond the limitations imposed by the FISC's orders. ER 595 ("NSA exceeded the scope of authorized acquisition continuously"), 601, 612 ("systemic overcollection"). NSA's violations of the FISC orders were "longstanding and pervasive" and amounted to "unauthorized electronic surveillance" that government officials knew or had reason to know of. ER 707, 700. NSA's overcollection was "sweeping and non-targeted." ER 702. "[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." ER 612-13.
- NSA's reporting to the FISC on the Internet metadata program was rife with misrepresentations. ER 603, 606-14, 664; ER 726-27 n.14.

- The NSA Draft OIG report confirms that AT&T participated in the Internet metadata program. ER 129, 133-34.

As with the bulk collection of call records, 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.

The government maintains that Internet metadata bulk collection focused on only certain categories of communications (including email metadata) and on international communications channels. ER 192-94, 199; ER 129, 132-34; ER 663, 673, 700. Yet even assuming that Internet metadata collection was limited to international communications, it is still more likely than not that each plaintiff had metadata collected by this program because plaintiffs regularly send international emails and engage in other international communications.

And the indeterminate, ever-changing, and essentially random nature of Internet communications routing means that wherever on the Internet backbone the Internet metadata collection devices may have been located, over the years it is more probable than not that at least one of each plaintiffs' communications passed through them. *See* ER 961, ¶2; ER 965-71, ¶¶21, 23, 26-30, 34-36; ER 973-75, ¶¶48-56; ER 982, ¶15; ER 984, ¶21; ER 986, ¶26; ER 989, ¶¶40, 42-43; ER 998, ¶25.

Additionally, any Internet metadata collection program is necessarily a content interception program. In order to collect the "to" and "from" email

addresses that the government characterizes as "metadata," it is necessary to reconstruct and examine the contents of the email message. ER 982-88, ¶¶12, 15-33, 38 (at ¶27: "there is no way to view or collect the "to" or "from" addressing information . . . without first reconstructing the email message content"); ER 965-66, ¶22(c); ER 976, ¶¶59-61. The email addresses are within the contents, not outside of it as with a physical letter. So any Internet metadata collection program is necessarily copying, at least temporarily, and examining the contents of the emails whose metadata it is collecting.

Because collecting Internet metadata requires first examining the contents of the email, the devices the NSA has used for Internet backbone surveillance, including the surveillance devices at AT&T's Folsom Street Facility, could also be used to collect Internet metadata. Indeed, the AT&T documents show that a "Meta Data Cabinet" was present in the SG3 room. ER 1284. If the Internet backbone surveillance devices at the Folsom Street Facility and elsewhere were also used to collect Internet metadata (something the classified evidence should show), then the same evidence that shows plaintiffs' standing to challenge Internet content surveillance also gives them standing to challenge Internet metadata collection.

E. The Undisclosed Classified Evidence Also Demonstrates Plaintiffs' Standing

The public evidence alone is sufficient to prove plaintiffs' standing.

But any classified evidence that supports plaintiffs' standing must also be considered. *Fazaga* makes clear that where section 1806(f) applies, the secret evidence is in the case for all purposes. *Fazaga*, 916 F.3d at 1236-38.

Given the vast volume of phone records and Internet metadata in the government's databases, plaintiffs expect the government found their phone numbers and Internet communications identifiers when it searched those databases as the Court required. That is direct and conclusive evidence of standing for those two programs.[15]

Additionally, plaintiffs are confident that, if the government properly responded to plaintiffs' discovery requests and to the district court's order to marshal all evidence relevant to standing, the undisclosed classified evidence includes the following categories of evidence supporting plaintiffs' standing. The district court's classified order also should address this evidence.

[15] Even if plaintiffs' phone records and Internet metadata are not currently in the government's databases, it is more likely than not they were at one time. While litigation was pending, and without district court authorization, the government destroyed all phone records covering May 2006 to sometime in 2009 (leaving only phone records for October 2001 to May 2006 and for sometime in 2009 to the program's end in November 2015) and destroyed all Internet metadata from July 2004 to the program's end in December 2011 (leaving only Internet metadata from October 2001 to July 2004). ECF Nos. 230 at ¶¶38-39, 228 at ¶31, 260 at 9.

Classified Evidence	Phone Records	Internet Content	Internet Metadata
Letters from the Attorney General or other officials to plaintiffs' communications providers during the PSP showing participation of plaintiffs' phone and Internet providers in phone records, Internet content, and Internet metadata programs.	X	X	X
FISC Orders showing participation of plaintiffs' phone and Internet providers in phone records, Internet content, and Internet metadata programs.	X	X	X
Government documents showing Internet content and metadata was collected by copying and processing Internet communications at AT&T's peering points and Internet backbone nodes.		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 Draft OIG Report and the AT&T documents.	X	X	X
Documents, including diagrams, evidencing participation in the programs by AT&T (including under the codename "Fairview") and Verizon (including under the codename "Stormbrew").	X	X	X

F. The District Court Erred In Denying Plaintiffs Access To The Classified Evidence

The district court abused its discretion in denying plaintiffs' counsel secure access to the classified evidence pursuant to section 1806(f) and subject to security clearances. *See* § 1806(f); *Fazaga*, 916 F.3d at 1251; ECF Nos. 393, 400, 401; ER 34.

Granting access to plaintiffs is "necessary to make an accurate determination of the legality of the surveillance." § 1806(f). In our adversarial system, the task of digesting raw evidence is the job of the parties, not the court. It is the parties that have the time and the resources to do so and, most importantly, understand the significance of facts and documents and their relationship to other evidence.

That is especially true given the thousands of pages of secret documents, the 193-page secret declaration, and the technological issues surrounding the government surveillance practices. The district court lacked the time, resources, and technical background to analyze this raw evidence and to integrate it with the other evidence. It compounded its challenge of digesting unaided the government's secret evidence by refusing to compel the government to respond to plaintiffs' RFAs with the clear admit-or-deny responses required by Rule 36, instead allowing the government to substitute narrative responses combining multiple interrogatories and RFAs. ECF Nos. 388, 389, 389-1, 389-2, 389-3, 411; ER 29.

Denying plaintiffs access also denied them the opportunity to challenge the secret evidence, either with rebuttal evidence or on admissibility grounds. The concern is not theoretical; the government has admitted to making multiple false, misleading, or grossly mistaken material statements in its secret filings with the district court and with the FISC. ER 603, 606-14; ER 715, 725-27 & nn.14, 15; ER 822; ER 427-28; ER 201-08; ECF Nos. 379-2, 386-2.

By refusing to grant access, the district court also denied plaintiffs access to its classified order. This has deprived plaintiffs of due process on appeal, putting them in the position of appealing a classified dispositive order whose holding, reasoning, factual findings, and supporting evidence are all kept from them.

On remand, the district court and the government should be instructed to grant access to cleared plaintiffs' counsel to any classified evidence, pursuant to sections 1806(f) and 2712(b)(4).

G. Plaintiffs' Claims Are Redressable

The district court's ruling that plaintiffs' claims are not redressable is fundamentally flawed and easily refuted. ER 21.

First, it is law of the case that plaintiffs' claims are redressable. "Jewel easily meets the third prong of the standing requirement. There is no real question about redressability. Jewel seeks an injunction and damages, either of which is an available remedy should Jewel prevail on the merits." 673 F.3d at 912.

Second, even if redressability were not law of the case, the test of redressability is whether a *favorable* decision applying sections 1806(f) and 2712(b)(4) to reject the state secrets privilege, deciding plaintiffs' claims on the merits in their favor, and awarding them damages and injunctive relief would offer them redress. It certainly would. *Clapper v. Amnesty International*, 568 U.S. 398, 409 (2013) ("redressable by a favorable ruling"). The district court asked the wrong question in asking whether an *unfavorable* decision dismissing plaintiffs' claims on state-secrets-privilege grounds without deciding the merits would offer plaintiffs redress. In doing so, it improperly conflated the state secrets privilege with Article III standing.[16]

Third, in enacting sections 1806(f) and 2712(b)(4) Congress has forbidden the district court from using the state secrets privilege to deny

[16] "[T]he redressability prong of the standing test is not an inquiry into the scope of the court's power to grant relief. . . . [T]he test *assumes* that a decision on the merits would be favorable and that the requested relief would be granted; it then goes on to ask whether that relief would be likely to redress the party's injury.

"In sum, the redressability test asks whether a plaintiff's injury would be likely to be redressed *if the requested relief were granted*. To analyze standing by asking whether the relief would be likely to be granted, as petitioners would have us do, would conflate the redressability test with a motion to dismiss for lack of jurisdiction. We examine below the petitioners' assertion that no relief is available in this case; we decline, however, to conduct that analysis under the rubric of standing doctrine." *In re Thornburgh*, 869 F.2d 1503, 1511 (D.C. Cir. 1989) (citations omitted).

plaintiffs relief, so the state-secrets barrier to redressability that the district court posited is nonexistent.

H. The Claims Against The Personal-Capacity Defendants Must Also Be Reinstated

The dismissal of the claims against the personal-capacity defendants must be reversed as well. The district court stayed the claims against them, and they did not move for summary judgment. The district court entered judgment in their favor only because it granted summary judgment to the government, and with the reversal of the judgment in the government's favor the judgment in their favor must be reversed as well. ER 27 n.4.

IV. Plaintiffs Are Entitled To Summary Judgment On Their Fourth Amendment Internet Interception Claim

Plaintiffs moved in 2014 for partial summary judgment on their Fourth Amendment Upstream Internet interception claim. In its 2015 order, the district court dismissed that claim for lack of standing and alternatively as barred by the state secrets privilege. ER 46. It reaffirmed the dismissal in its 2019 order. ER 22 n.3. Both of these grounds are erroneous for the reasons stated in sections II and III above. Plaintiffs are entitled to partial summary judgment on this claim because the undisputed evidence shows their Fourth Amendment rights have been violated.

A. Upstream's Mass Surveillance Of Internet Communications

As the PCLOB concluded, "[n]othing comparable [to Upstream surveillance] is permitted as a legal matter or possible as a practical matter

with respect to analogous but more traditional forms of communication." ER 519.

As explained in section III(C) above, in its Upstream surveillance the government intercepts and searches Internet communications in bulk as they flow through junctions between Internet backbone networks, including the peering links on AT&T's Internet backbone. The communications stream transiting the Internet backbone includes all varieties of Internet activities, including email, live chat, and Internet telephone and video calls, as well as activities such as web browsing, video watching, social media, and search queries and results.

Plaintiffs have divided the Upstream surveillance process into four stages for ease of discussion of the additional facts relevant to the merits of their Fourth Amendment claim.

At stage one, the communications transiting domestic Internet backbone junctions are intercepted. ER 404, 432-34, 436, 439, 521. All of the communications flowing through the intercepted Internet backbone junctions are copied, a necessary step to enable them to be filtered and searched at later stages. ER 1213-14, ¶¶21-34; ER 1220, 1241, 1245, 1250, 1255, 1280, 1284, 1293-94, 1322-23, 1326-27; ER 1047-52, ¶¶56-58, 62, 70-73, 77; ER 1060-61, ¶109; ER 1197-98, ¶6; ER 1200-04, ¶¶10-12, 15, 19-23.

At stage two, the copied communications are imperfectly filtered in an attempt to eliminate wholly domestic communications and leave only

communications in which at least one end is located outside the United States. ER 433-36, 438, 517. This filtering intentionally retains communications between Americans and persons located abroad. *Id*. Moreover, this imperfect filtering does not exclude all wholly domestic communications, resulting in a significant number of domestic communications in the filtered communications stream that is subsequently searched. *Id*.[17]

At stage three, the contents of the filtered communications are searched for designated selectors. ER 433-34. The entire contents are searched, top to bottom.[18] As the PCLOB explains, "[d]igital

[17] The ineffectiveness of geographic Internet Protocol filters is one reason why the government's filtering fails to exclude all domestic communications. ER 435; ER 1061-62, ¶¶110-12. Another reason is that because the Internet sends communications on unpredictable and everchanging pathways, a communication between two domestic parties can follow a path that takes it outside the United States for part of its journey. ER 438; ER 965-68, ¶¶21, 25-30; ER 973-74, ¶¶48, 52; ER 977-78, ¶64. Another reason is that websites, cloud servers, and Internet services that appear to be domestic may be located anywhere in the world unbeknownst to the user. ECF No. 262, Ex. F. In addition, providers of domestic Internet services back up and store user emails and data on servers around the world. ER 996, ¶16; ER 997-98, ¶¶22-25; ER 977-78, ¶64.

[18] "If the NSA therefore applied its targeting procedures to task [i.e., to use as a selector] email address 'JohnTarget@example.com,' to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message." ER 434.

(footnote continued on following page)

communications like email . . . enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." ER 519. The government refers to communications whose message body contain a reference to a selector, as opposed to being "to" or "from" a selector, as "about" communications. ER 404, 434, 518-19.

These searches are suspicionless: "[T]he government's collection devices examine the *contents* of the communications, without the government having held any prior suspicion regarding that communication." ER 520.

The filtered communications that are searched include the international Internet communications of plaintiffs and other Americans, as well as many wholly domestic communications as previously noted.

Because the government searches the contents of the entire post-filtering communications stream, hundreds of millions of communications are searched that do *not* contain any selectors, along with the relative few that do. Those communications that are searched and found not to contain any selectors are the communications of millions of innocent Americans,

---

(footnote continued from previous page)
See also ER 404, 430, 436, 481, 518-19 ("NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it"); ER 1052-55, ¶¶75, 82-85; ER 1204, ¶23.

including plaintiffs, with no connection to any surveillance target and whom the government does not suspect of any wrongdoing.

At stage four, communications containing selectors are deposited into government databases for retention. ER 434, 508 n.476. The communications the government permanently retains are not at issue here.[19]

Until April 2017, the government retained communications that had a selector anywhere within them, i.e., that were to, from, or about a designated selector. Fn. 18, *supra*; ER 434. In April 2017, after repeatedly violating the FISC's orders limiting the use of "about" communications it retained, the government voluntarily ceased retaining "about" communications. ECF No. 358-1 at 4-5, 25. But it is still searching the contents of the filtered communications, because the contents of an email include both the body of the message and the "to" and "from" addresses.[20] ER 982, ¶12; ER 986-87, ¶¶27, 33; ER 965-66, ¶22(c); ER 976, ¶¶59-61.

[19] The district court got it wrong when it asserted that plaintiffs' motion claimed that "all of their Internet communications have been collected and amassed in storage." ER 51. Plaintiffs' motion challenged only the initial seizure and searching of their communications, not storage. ECF No. 261 at 8-9. Permanent retention of the thing seized or searched is never required for a Fourth Amendment claim.

[20] The "to" and "from" addresses are not used to route the email between the sender's and the receiver's mail servers as the email transits the Internet; instead, they are part of the contents inside the "envelope" with the message body. ER 982-87, ¶¶15-33; ER 966-67, ¶¶25-27.

Plaintiffs challenge the constitutionality of wholesale seizure of the stream of Internet communications, and the subsequent searching of the filtered communications for selectors. As explained in section III(C), AT&T is one of the Internet backbone providers whose communications the government intercepts and searches. As the government concedes and as the experts explain, plaintiffs' communications have passed through the peering links that AT&T copies with splitters and sends to the SG3 room. They have also passed through many other Internet backbone junctions. ER 974, ¶52; ER 977, ¶64. And the government's filters are designed to permit the international communications of plaintiffs to pass through to the searching stage.

The government has suggested that the technical implementation of Upstream surveillance has evolved over time. Any such changes do not fundamentally alter plaintiffs' claim. This is because, given that the purpose of Upstream surveillance is to search for selectors in the undifferentiated mass of communications flowing through Internet backbone junctions, by its nature that process will involve some form of copying (to avoid unacceptable performance degradation of the providers' Internet services) and content searching (because the "to" and "from" addresses of an email are inside the message, not on its "envelope"). ER 982, ¶12; ER 984-89, ¶¶22, 27, 33, 38; ER 992, ¶56; ER 965-66, ¶22; ER 976, ¶¶59-61.

B. The Government's Warrantless, Suspicionless, Mass Searches And Seizures Of Plaintiffs' Internet Communications Violates The Fourth Amendment

1. The Fourth Amendment Protects Plaintiffs' Internet Communications

The Fourth Amendment is a fundamental guarantee of personal privacy whose "basic purpose" "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 528 (1967). The Founders "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone . . . ." *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

"[O]ur cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against 'arbitrary power.' Second, and relatedly, that a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.' [¶] We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Carpenter*, 138 S. Ct. at 2214 (citations omitted).

Protecting privacy in personal communications like plaintiffs' Internet communications is one of the core principles of the Fourth Amendment. It expressly protects a person's right to be "secure" in their "papers" and "effects" from government intrusion. U.S. Const. amend. IV. It "embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *U.S. v. Jones*, 565 U.S. 400, 406 (2012).

The Founders' special protection for papers and effects stems from their determination to prohibit the indiscriminate, suspicionless rummaging and seizure of papers that the English Crown had conducted using "general warrants"—warrants that failed to specify the papers that were sought, the person whose papers could be searched and seized, or the place to which the search was confined. *Carpenter*, 138 S. Ct. at 2213; *Riley v. California*, 573 U.S. 373, 403 (2014); *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965); *Marcus v. Search Warrants of Property*, 367 U.S. 717, 726-29 & n.22 (1961).

"The immediate object of the Fourth Amendment was to prohibit the general warrants and writs of assistance that English judges had employed against the colonists." *Virginia v. Moore*, 553 U.S. 164, 168-69 (2008); *accord Payton*, 445 U.S. at 583. "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403.

Plaintiffs' Internet communications fall within the Fourth Amendment's categorical protections for "papers" and "effects," which protects a person's information in digital as well as physical form: "The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities." *Cotterman*, 709 F.3d at 957. Thus, digital communications "implicate[] the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers.' The express listing of papers reflects the Founders' deep concern with safeguarding the privacy of thoughts and ideas—what we might call freedom of conscience—from invasion by the government." *Id*. at 964 (citations and internal quotation marks omitted); *accord Berger v. New York*, 388 U.S. 41, 51 (1967).

Even apart from the Fourth Amendment's specific protection of "papers" and "effects," plaintiffs' electronic communications are protected because plaintiffs have a reasonable expectation of privacy in them.[21] *Cotterman*, 709 F.3d at 964-65 (electronic communications "are expected to be kept private and this expectation is 'one that society is prepared to recognize as reasonable'"); *In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016); *U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), *cited with approval in Carpenter*, 138 S. Ct. at 2222; *id.* at 2230

[21] The "reasonable expectation of privacy test" is the alternative test for the scope of Fourth Amendment protections. *See Jones*, 565 U.S. at 406, 411; *id*. at 414 (Sotomayor, J., concurring); *id*. at 422-32 (Alito, J., concurring).

(Kennedy, J., dissenting); *id.* at 2262, 2269 (Gorsuch, J., dissenting); *see also U.S. v. U.S. District Court (Keith)*, 407 U.S. 297, 313 (1972); *Katz v. U.S.*, 389 U.S. 347, 353 (1967); *id*. at 361 (Harlan, J. concurring).

The Fourth Amendment privacy interests in digital information that the Supreme Court recognized in *Riley* and *Carpenter* are fully applicable to the Internet communications of plaintiffs that the government is seizing and searching and trigger the warrant requirement. *Carpenter*, 138 S. Ct. at 2219, 2221-22; *Riley*, 573 U.S. at 403. In *Riley*, the Court specifically noted the protected privacy interests in Internet browsing and explained how the breadth and depth of a person's digital information gives a wide-ranging picture of a person's most private thoughts and actions—even beyond what a general search of their home might reveal. *Id.* at 393-98.

Moreover, the Fourth Amendment fully protects plaintiffs' Internet communications while in transit. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (letters in transit can only be opened and examined with a warrant); *Hearst v. Black*, 87 F.2d 68, 70-71 (D.C. Cir. 1936) (government's en masse copying of telegrams in transit was a "dragnet seizure" that violated sender's possessory and privacy rights).

2. Stage One: The Government's Mass Interception And Copying Of Internet Communications Is A Seizure

The government's interception and copying of the contents of the Internet activities of plaintiffs and millions of other Americans at the

Internet backbone facilities of AT&T—stage one of the government's surveillance described in section IV(A) above—is a seizure.

A seizure occurs when there is a meaningful interference with a possessory interest. *Jones*, 565 U.S. at 408 n.5; *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984). Plaintiffs have a possessory interest and a privacy interest in their Internet communications and in the information those communications contain, as the government conceded below. 12/19/14 RT 75:19-24. The exercise of dominion and control by the government is one type of meaningful interference that results in a seizure. *Jacobsen*, 466 U.S. at 120-21 & n.18.

Copying plaintiffs' communications is a seizure because it is an exercise of dominion and control that meaningfully interferes with their possessory interests in their communications. *See Berger*, 388 U.S. at 59-60 (making an electronic copy of an oral conversation was a seizure of the conversation); *Katz*, 389 U.S. at 353 (same); *Hearst*, 87 F.2d at 70-71 (dragnet copying of telegrams interfered with possessory and privacy interests in the telegrams).

Below, the government argued that its seizure and searching of plaintiffs' communications lasted only an instant and was too brief to trigger the Fourth Amendment. There is no evidence in the record supporting the contention that its seizures last only an instant.

In any event, duration is not the relevant measure of interference. The fact that technology may now permit the government to copy

instantaneously all of plaintiffs' communications and expose them to its full scrutiny for equally instantaneous searching does nothing to diminish the scope of its interference. The right to exclude others is a fundamental possessory interest, and plaintiffs' right to exclude the government from their communications is completely violated when all of the information in their communications is copied in a form that makes it fully available for top-to-bottom searching, and when this copying goes on continuously for many years, regardless of the duration of any particular seizure.

3. Stage Three: The Government's Examination Of The Contents Of Plaintiffs' Internet Communications Is A Search

The government's content-searching of plaintiffs' Internet communications after it seizes them—stage three of the government's surveillance described in section IV(A) above—is a search. "When the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred." *Florida v. Jardines*, 569 U.S. 1, 5 (2013) (citation and internal quotation marks omitted); *Jones*, 565 U.S. at 404-07 & n.3 (same). The government physically intrudes into plaintiffs' digital communications when it searches them from top to bottom looking for its selectors.

The government's content-searching is also a search under a reasonable-expectation-of-privacy analysis. As explained above, plaintiffs

have a reasonable expectation of privacy in their emails and other electronic communications. "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213.

4. The Warrantless Seizure And Searching Of Plaintiffs' Internet Communications Is Unconstitutional

The seizures and searches of plaintiffs' communications conducted as part of Upstream's mass surveillance are unconstitutional because they are conducted without a warrant and without any suspicion of plaintiffs or their communications. *Katz*, 389 U.S. at 353, 356-59; *Berger*, 388 U.S. at 55-64; *Warshak*, 631 F.3d at 286-87; *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986).

Like other "papers" and "effects," plaintiffs' electronic communications can only be seized and searched with a warrant issued by a neutral and detached magistrate, supported by probable cause and describing with particularity the location of the search and the communications to be seized. *See Ex parte Jackson*, 96 U.S. at 733. National security does not excuse the need for a warrant to seize or search plaintiffs' communications. *Halperin*, 807 F.2d at 185.

Warrants are not a dusty formalism but *the* time-tested method for protecting Americans' privacy against government intrusion. "Our cases

have historically recognized that the warrant requirement is an important working part of our machinery of government, not merely an inconvenience to be somehow weighed against" the government's interest in proceeding without a warrant. *Riley*, 573 U.S. at 401 (internal quotation marks omitted).

The warrant's probable cause requirement ensures that no search or seizure occurs where there is less than probable cause or, worse, no suspicion at all. *Keith*, 407 U.S. at 316 ("The further requirement of 'probable cause' instructs the magistrate that baseless searches shall not proceed."); *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (same). It also serves to limit the scope of the search. *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9th Cir. 1991).

The warrant's particularity requirement ensures that "those searches deemed necessary [are] as limited as possible." *Coolidge*, 403 U.S. at 467. The "need for particularity" "is especially great in the case of [electronic] eavesdropping" because it "involves an intrusion on privacy that is broad in scope." *Berger*, 388 U.S. at 56. Particularity ensures that "the search will be carefully tailored to its justifications," eliminating the threat of "general searches." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The particularity requirement also makes general searches "impossible" by ensuring that when it comes to what can be searched or seized, "nothing is left to the discretion of the officer executing the warrant." *Marron v. U.S.*, 275 U.S. 192, 195-96 (1927); *see also Berger*, 388 U.S. at 49-50, 56, 58-59; *Katz*, 389 U.S. at 358-59.

Judicial warrants founded on particularity and probable cause are crucial in electronic surveillance because those searches and seizures occur without leaving a trace. *See Keith*, 407 U.S. at 313, 318. This concern is heightened in the case of mass surveillance, where the overwhelming majority of the Americans whose communications are seized and searched are not even suspected of a crime or of being an agent of a foreign power.

No warrant could justify the mass, suspicionless seizures occurring here because they are general seizures occurring without probable cause or particularity. They are the modern-day equivalent of the hated general warrants that the Fourth Amendment was meant to stamp out forever. They are unconstitutional because they amount to "a virtual, all-encompassing dragnet of personal papers and property to be seized at the discretion of the State." *U.S. v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003). It was precisely this power to seize papers and effects indiscriminately, in bulk, and without particularized suspicion that made general warrants objectionable as "totally subversive of the liberty of the subject." *Marcus*, 367 U.S. at 728-29 (citation omitted).

Similarly, the government's warrantless and suspicionless indiscriminate searching of the communications of plaintiffs and millions of others is an unconstitutional general search that no warrant could properly authorize. It is the "general, exploratory rummaging" that the Fourth Amendment prohibits. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (citation omitted). The Fourth Amendment "protect[s] against all general

searches. Since before the creation of our government, such searches have been deemed obnoxious to fundamental principles of liberty." *Go-Bart Importing Co. v. U.S.*, 282 U.S. 344, 357 (1931).

V. Upstream Evidentiary Discussion

This Upstream Evidentiary Discussion lays out in greater detail the evidence supporting plaintiffs' standing for their Upstream Internet interception claims.

1. Evidence From AT&T And Its Employees

a. Klein's Testimony

AT&T employee Mark Klein operated the splitters and diverted the copied communications to the SG3 room.

Klein was in charge of the Internet room at AT&T's Folsom Street Facility in San Francisco. The Internet room contains AT&T's Internet backbone circuits—the fiber-optic cables and switches carrying AT&T's Internet traffic, including communications to or from AT&T's customers. ER 1211-13, ¶¶15, 19-22.

The Internet room also contains the peering links. ER 1213-14, ¶¶22, 29-33. The peering links carry domestic and international communications of AT&T customers, as well as communications of users of non-AT&T networks connected to the peering links. ER 1212, ¶19; ER 1214, ¶¶29-34; ER 1047-52, ¶¶62, 70-73, 77; ER 1057-59, ¶¶96-104.

To divert to the NSA the Internet communications traveling between its backbone network and other providers' networks, AT&T connected the

fiber-optic cables of the peering links to a "splitter cabinet" installed in the Internet room. ER 1213-14, ¶¶22-34; ER 1327. Klein was responsible for maintaining the fiber-optic circuits in the Internet room, including the peering-link circuits, and for physically connecting new circuits to the splitter cabinet. ER 1212-15, ¶¶19-22, 29, 36.

Internet communications are carried as light signals on fiber-optic cables. ER 1213, ¶¶21-23. The splitter cabinet splits the light signals in two, making two identical copies of all of the communications carried on the peering links. ER 1213, ¶¶23-25. The splitter cabinet diverts one copy of each communication into the NSA-controlled SG3 room via fiber-optic cables linking the splitter cabinet to the SG3 room, while allowing the other copy to travel its normal course over the Internet to its intended destination. ER 1213-14, ¶¶25-34.

In the course of consulting with another AT&T technician while connecting new circuits to the splitter cabinet, Klein learned that AT&T had similar splitter cabinet installations in other cities, including Seattle, San Jose, Los Angeles, and San Diego. ER 1215, ¶36.

In the course of performing his job duties, Klein observed the NSA's control of the SG3 room operations. AT&T management emailed Klein telling him to expect a visit by an NSA agent; Klein's manager told him the NSA agent was coming to interview a colleague ("FSS #2") for a "special job." ER 1210-11, ¶¶8-10.

Klein observed the NSA agent come and meet with FSS #2, and afterwards Klein's manager told him that FSS #2 was assigned the NSA special job. ER 1210-11, ¶¶8-10. Klein later observed FSS #2 installing equipment in the high-security SG3 room. ER 1211, ¶¶10-14.

Klein's manager subsequently told Klein that an NSA agent would again come to discuss another colleague's (FSS #3) suitability to take over the NSA special job from FSS #2. ER 1212, ¶16. Klein observed the NSA agent come and meet with his manager. *Id*. FSS #3 took over the NSA special job from FSS #2 and operated the SG3 room. ER 1212, ¶¶16-17.

The AT&T employees in charge of the SG3 room had NSA security clearances, and no other persons were permitted in the room. ER 1211-12, ¶¶14, 17-18. Klein knew that the only reason he was denied access to the SG3 room was that he lacked an NSA security clearance. *Id*.

b. The AT&T Documents Show The Splitters, The Peering Links, And The Spy Equipment In The SG3 Room

Klein's declaration includes three AT&T documents he used in performing his job of maintaining the splitter cabinet and the peering-link circuits and SG3 room circuits attached to it. ER 1211-15, ¶¶15, 20, 25, 27-36.

Two documents (Exhibits A and B) describe "how to connect the already in-service circuits to a 'splitter cabinet.'" ER 1213, ¶¶25-26; ER

1216-80. Exhibit B lists the peering-link circuits that the splitter copied and diverted to the SG3 room. ER 1280.

Exhibit A also identifies Atlanta as an additional AT&T location with splitter cabinets. ER 1233; *see* ER 1062-63, ¶¶113-118.

The third AT&T document (Exhibit C), "described the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor." ER 1214, ¶28; ER 1281-1339. This document also "listed the equipment installed in the SG3 Secure Room," including a Data Filter Cabinet and a Narus "Semantic Traffic Analyzer" capable of filtering, searching, and analyzing communications—the processes Upstream performs on the communications stream flowing across peering links. ER 1214-15, ¶35; ER 1284; ER 1052-56, ¶¶75-88.

As plaintiffs' experts explain, Exhibit C shows that the SG3 room contains equipment designed to perform the filtering and searching described by the PCLOB of the redirected copies of Internet communications, 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 via the secret "SG3 backbone." ER 1284; ER 1203-04, ¶22; ER 1050-56, ¶¶68, 70-77, 79-85, 88; ER 972-73, ¶45.

c. Adverse Witness Russell Confirms The Information In The AT&T Documents And The Klein And Marcus Declarations

James Russell, AT&T's Managing Director-Asset Protection, attested that Klein's declaration, the AT&T documents, and the expert declaration of J. Scott Marcus all accurately describe the spy equipment present within the SG3 room and the Internet room, AT&T's Internet backbone network and the peering links connecting it to other providers' networks, the splitter cabinet and its connections to the peering links and the SG3 room, and AT&T's Folsom Street Facility. ER 1197-98, ¶1, 4-6; ER 1200-04, ¶¶10-12, 15, 19-23. In doing so, Russell does not just authenticate the AT&T documents; he independently attests from his own knowledge to the truth of facts stated in the AT&T documents and the Klein and Marcus declarations. *Id*.

Russell attests to the facts that the AT&T documents and the Klein and Marcus declarations disclose about "the building [i.e., the Folsom Street Facility] in which Internet backbone facilities of AT&T and others are located and interconnected [i.e., the peering links], the physical locations within the building in which particular equipment is located, the specific cabinets that house this equipment, [and] the manufacturers and models of the equipment." ER 1197-98, ¶6. "These documents list equipment manufacturers, equipment types and even specific model numbers of equipment deployed in the San Francisco building, for example. They list specific circuit IDs and the peering partners with which we interconnect

through these circuits. And they provide detailed circuit design and equipment deployment diagrams and descriptions." ER 1201-02, ¶15.

Russell attests that the SG3 room spy equipment described by Exhibit C and analyzed by Marcus is actually present in the SG3 room, including the Narus Semantic Traffic Analyzer, the Narus Logic Analyzer, and the secret "SG3 backbone" cable providing secure communication to and from the surveillance equipment in the SG3 room. ER 1201-04, ¶¶15, 19-23; ER 1214-15, ¶35; ER 1284, 1287, 1293, 1323; ER 1049-53, ¶¶63, 68, 74-77, 79; ER 1055-56, ¶¶86-89; ER 1197-98, ¶6. Russell states Exhibit C "identifies the manufacturers and product names and numbers for many pieces of equipment" and "the Marcus Declaration describes a specific San Francisco AT&T location and types of equipment contained in that building." ER 1203-04, ¶¶22-23.

d. Long's Testimony

AT&T employee Phillip Long attests that he was directed to shut down existing AT&T Internet backbone connections in California and instead reroute all Internet backbone traffic through the Folsom Street Facility, even though there was no business or engineering reason to do so. ER 956-59, ¶¶9-20, 25. The absence of any commercial or engineering purpose to AT&T's centralization of Internet traffic in the Folsom Street Facility supports the inference that it was a surveillance location.

Long corroborates that AT&T restricted access to the SG3 room (Room 641A), contrary to its normal practices. ER 958, ¶21. Long also was

instructed to connect a large fiber-optic cable outside the SG3 room to one coming from inside the room without any identification of the equipment within the SG3 room to which the cable was attached, contrary to AT&T's normal engineering practices but consistent with the existence of the secret "SG3 backbone." ER 958, ¶22.

2. Expert Evidence: Marcus, Reid, Blaze and Soltani

J. Scott Marcus's decades of telecommunications experience includes providing Internet backbone services to AT&T. ER 1037-41, ¶¶7-29. Marcus also served as the Senior Advisor for Internet Technology to the Federal Communications Commission. ER 1040, ¶24.

Marcus analyzes and explains in detail the technical capabilities of splitter equipment and the spy devices in the SG3 room. ER 1045-62, ¶¶44-112.

Marcus explains that a fiber-optic splitter is not a selective device; all traffic on the split circuit is copied and diverted, including both domestic and international communications. ER 1050-51, ¶¶70-73; ER 1058-61, ¶¶99-109.

Marcus explains how the internal evidence of the AT&T documents supports the conclusion that multiple surveillance locations exist. ER 1062-63, ¶¶113-18.

Marcus "conclude[s] that AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of [Internet Protocol]-

based communications information." ER 1043, ¶38. Marcus concludes it is "highly unlikely" that AT&T would have constructed the surveillance infrastructure for its own benign commercial purposes. ER 1043-46, ¶¶40-49; ER 1065-69, ¶¶128-47. He concludes instead that it is "highly probable" that the purpose of the equipment is government surveillance. ER 1046, ¶49; ER 1065, ¶128.

Dr. Brian Reid is an Internet network engineering expert, including serving as Google's Director of Operations. He analyzes the splitter technology and provides information on the transmission of Internet communications. ER 966-76, ¶¶24-58. He confirms the splitter "copies all traffic passing over all of the peering-link fibers." ER 965, ¶22(a); ER 972, ¶42.

He concludes 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" and that it is "highly likely that plaintiffs' communications traveled through the peering links." ER 973-74, ¶¶48, 50-51.

Matthew Blaze is a Georgetown University computer science professor. He provides background information on the transmission of Internet communications. ER 982-87, ¶¶15-33. He analyzes the splitter infrastructure and how it dovetails with the government's disclosures of its surveillance activities. ER 988-92, ¶¶34-57. He confirms that a splitter "copies all the traffic on the original link." ER 988, ¶34.

Professor Blaze states, given how the Internet routes a communication to its destination, "[i]t is highly likely that the communications of all plaintiffs passed through the link connected to the splitter (and thus the splitter itself)." ER 989, ¶¶39, 41-43.

Ashkan Soltani is the former Chief Technologist for the Federal Trade Commission. ER 994, ¶3. He was part of the *Washington Post* team that won a 2014 Pulitzer Prize for its reporting on NSA surveillance. ER 995, ¶9. Soltani explains yet another reason why plaintiffs' communications were likely intercepted by Upstream surveillance.

Plaintiffs are users of Gmail and Yahoo email (which provides the AT&T-branded email services used by AT&T customers). ER 1001-02, ¶¶16, 19 (Gmail, Yahoo email); ER 1008, ¶12 (Gmail); ER 1016, ¶¶14-15 (Gmail, Yahoo email); ER 1021, ¶¶15, 17 (Gmail, Yahoo email). Gmail and Yahoo are constantly shipping back-up copies of customer emails over the Internet between their data centers (both within the U.S. and abroad) in a process that is completely independent of whether the customer is sending an email. ER 994, ¶2; ER 996-98, ¶¶16-18, 21-25. Because these shipments are constantly traversing the Internet, the NSA's Internet backbone interception devices are likely to intercept these email shipments regardless of where those devices are located. ER 996, ¶16; ER 998, ¶25.

3. Plaintiffs' Use Of Internet Services

Plaintiffs use the Internet to communicate both domestically and internationally, including sending and receiving emails and visiting

websites. ER 1000-02, ¶¶7-21; ER 1007-09, ¶¶5-17; ER 1013, ¶¶8-9; ER 1015-17, ¶¶8-19; ER 1020-22, ¶¶6-19. Plaintiffs engage in email correspondences with individuals in such countries as Saudi Arabia, Indonesia, Australia, New Zealand, Holland, Denmark, South Africa, Taiwan, Canada, France, Germany, the United Kingdom, China and Spain, as well as visiting foreign websites. ER 1000-01, ¶¶9-10, 16; ER 1016-17, ¶¶11, 18; ER 1021-22, ¶¶9, 18; ER 1008-09, ¶¶11, 16-17.

Plaintiffs are California residents, and all plaintiffs except plaintiff Hepting are AT&T Internet customers. ER 1000, ¶¶1, 3-5; ER 1004; ER 1007, ¶1; ER 1013, ¶¶2, 7; ER 1015, ¶¶1, 3-7; ER 1018; ER 1020, ¶¶1, 3-5; ER 1024. The Internet backbone circuits that the splitters copy carry the communications of plaintiffs and other AT&T customers, as well as non-AT&T customers like plaintiff Hepting. ER 1008-09, ¶¶13-17; ER 1050-52, ¶¶70-73; ER 1058-61, ¶¶100-109; ER 965, ¶21; ER 973-74, ¶¶48, 50-51; ER 989-90, ¶¶39-46.

CONCLUSION

The judgment should be reversed and remanded with directions to enter partial summary judgment for plaintiffs on their Fourth Amendment Internet interception claim, and to proceed with discovery on the merits and trial using the procedures of section 1806(f) and section 2712(b)(4).

Dated: September 6, 2019 Respectfully submitted,

s/ *Richard R. Wiebe*

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKEY
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION

THOMAS E. MOORE III
ROYSE LAW FIRM

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

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs-Appellants

CONSTITUTIONAL AND STATUTORY ADDENDUM

U.S. Constitution, amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

18 U.S.C. § 2712, subsections (a) & (b)

18 U.S.C. § 2712 Civil actions against the United States

(a) In General.—
Any person who is aggrieved by any willful violation of this chapter [the Stored Communications Act] or of chapter 119 of this title [the Wiretap Act] or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages—

> (1) actual damages, but not less than $10,000, whichever amount is greater; and
> (2) litigation costs, reasonably incurred.

(b) Procedures.—

> (1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.
>
> (2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final

denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

50 U.S.C. § 1806(f)

50 U.S.C. § 1806(f) In camera and ex parte review by district court.

Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such

other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT
Form 8. Certificate of Compliance for Briefs

9th Cir. Case Number(s) 19-16066

I am the attorney or self-represented party.

This brief contains 19,614 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[ ] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
[ ] it is a joint brief submitted by separately represented parties;
[ ] a party or parties are filing a single brief in response to multiple briefs; or
[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[X] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature: ___*s/Richard R. Wiebe*_____ **Date:** September 6, 2019

STATEMENT OF RELATED CASES

Fazaga v. FBI, 916 F.3d 1202 (9th Cir. 2019), resolved issues regarding the scope and application of 50 U.S.C. § 1806(f) relevant to this case. A petition for rehearing or rehearing en banc is pending as of the time of filing of this brief.