CASE NO. 15-16133
(PRIOR APPEAL: NO. 10-15616)

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, ERIK KNUTZEN, 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

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

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 813-9700

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
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
MARK RUMOLD
ANDREW CROCKER
JAMIE L. WILLIAMS
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

INTRODUCTION

"Indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980). To that end, the Fourth Amendment protects "[t]he right of the people to be secure in their . . . papers, and effects, against unreasonable searches and seizures."

This appeal seeks a judicial determination of whether this core purpose—providing Americans with security against indiscriminate seizures and searches of their papers and effects—is violated when the government copies and searches 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 result is a digital dragnet—a technological mass surveillance system that subjects millions of ordinary Americans to the seizure and searching of their online correspondence, conversations, searches, reading and other activities. The content of those online activities, as the Supreme Court noted, is "as diverse as human thought," *Reno v. A.C.L.U.*, 521 U.S. 844, 852 (1997), encompassing personal, medical, religious, associational, political, and familial matters, from the mundane to the most sensitive.

At issue in this appeal is not only the constitutionality of this mass surveillance, but also whether plaintiffs have proven their standing to challenge the surveillance and whether section 1806(f) of title 50 U.S.C.

displaces the state secrets privilege in this lawsuit and requires the courts to decide the merits of plaintiffs' claim.

Plaintiffs claim that the government's mass interception, copying, and searching of their Internet communications violates their Fourth Amendment rights. On cross-motions for summary judgment on plaintiffs' Fourth Amendment Internet interception claim, the district court erroneously granted summary judgment in favor of the government defendants on two alternative grounds.

First, the court erred in concluding plaintiffs lacked standing. Plaintiffs' evidence, including extensive government admissions, shows that at least some of their Internet communications have been intercepted, copied, and searched, thus establishing their injury and giving them standing. Moreover, because the government defendants put in no evidence creating a genuine factual dispute regarding plaintiffs' standing, plaintiffs are entitled to summary judgment on standing.

Second, the court erred in holding that the state secrets privilege barred any attempt by plaintiffs to litigate their claim. Congress has displaced the state secrets privilege in electronic surveillance cases like this one with the statutory procedure of section 1806(f) of title 50 U.S.C. Under section 1806(f), a claim of unlawful surveillance implicating secret evidence is decided on the merits, not dismissed.

Above all, the evidence demonstrates that plaintiffs are entitled to summary judgment on the merits of their Fourth Amendment claim. The

suspicionless, warrantless interception and copying of plaintiffs' Internet communications is an unconstitutional seizure, and the subsequent content searching of some of those communications is an unconstitutional search.

STATEMENT OF JURISDICTION

The district court had jurisdiction over plaintiffs' Fourth Amendment Internet interception claim under 28 U.S.C. § 1331.

The district court entered final judgment on plaintiffs' Fourth Amendment Internet interception claim pursuant to Federal Rule of Civil Procedure 54(b). ER 1, 3. This Court has jurisdiction under 28 U.S.C. § 1291 over the district court's judgment.

The appeal is timely. Fed. R. App. Pro. 4(a)(1)(B). The district court entered judgment on May 21, 2015. ER 1. Plaintiffs appealed on June 4, 2015. ER 41.

STATEMENT OF FACTS

Plaintiffs and class representatives Carolyn Jewel, Erik Knutzen, and Joice Walton are AT&T Internet service subscribers.[1] Each of them relies on the Internet to send and receive personal and professional emails, to stay in touch with friends and loved ones, and to conduct private activities including web browsing and social media.[2] Additionally, like many other

[1] ER 113 (Jewel Decl.) at ¶¶ 2-3; ER 110 (Knutzen Decl.) at ¶¶ 2-3; ER 107 (Walton Decl.) at ¶¶ 2-3.

[2] ER 113 (Jewel Decl.) at ¶¶ 4-5, ER 110 (Knutzen Decl.) at ¶¶ 4, 6; ER 107 (Walton Decl.) at ¶¶ 4, 6.

Internet users, each plaintiff routinely communicates by email with persons outside the United States, and each visits websites that are hosted abroad.[3]

The government has made extensive admissions about its Internet surveillance activities, including the July 2014 *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* by the Privacy and Civil Liberties Oversight Board ("PCLOB Report").[4] These admissions show the government is intercepting and searching Internet communications in bulk as they flow through major fiber-optic network junctions on the Internet "backbone."[5] Almost all Internet traffic travels at some point over the Internet backbone—high-capacity, long-distance fiber-optic cables controlled by major Internet

[3] ER 113-14 (Jewel Decl.) at ¶¶ 6, 8; ER 110-11 (Knutzen Decl.) at ¶¶ 8, 9; ER 107-108 (Walton Decl.) at ¶¶ 7, 9.

[4] PCLOB is an independent agency in the executive branch charged with reviewing anti-terrorism activities for their impact on privacy and civil liberties. 42 U.S.C. § 2000ee. The PCLOB Report contains an extensive discussion of the government's Internet backbone surveillance activities. Plaintiffs may use statements in the PCLOB Report as admissions by a party-opponent. Fed. R. Evid. 801(d)(2).

[5] *See, e.g.*, ER 120, 124-26, 59, 105 (PCLOB Report); ECF No. 227 at ¶ 38, p. 25:14-16 (12/20/13 NSA Deputy Dir. Fleisch Classified Decl.) ("NSA collects electronic communications with the compelled assistance of electronic communications service providers as they transit Internet 'backbone' facilities within the United States"); ER 159 (The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act) ("NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States").

providers such as AT&T.[6] 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, and search queries and results. The government describes its Internet backbone seizures and searches as "Upstream" collection.[7]

The PCLOB Report describes the overall surveillance process, which plaintiffs have divided into four stages for ease of discussion:

> Once tasked, selectors used for the acquisition of upstream Internet transactions[8] 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. To identify and acquire Internet transactions associated with the Section 702-tasked selectors on the Internet backbone, Internet

---

[6] ER 217-18 (Marcus Decl.) ¶¶ 12-14 & n.5; ER 257-58 (Klein Decl.) ¶¶ 22, 29-34.

[7] ER 120, 124 (PCLOB Report).

[8] In the NSA's parlance, a "transaction" is a single communication or a group of communications: "While the NSA's upstream collection is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*. . . . An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet. An Internet transaction could consist of a single discrete communication, such as an email that is sent from one server to another. . . . In other instances, however, a single Internet transaction might contain multiple discrete communications." ER 59 (PCLOB Report) (italics original).

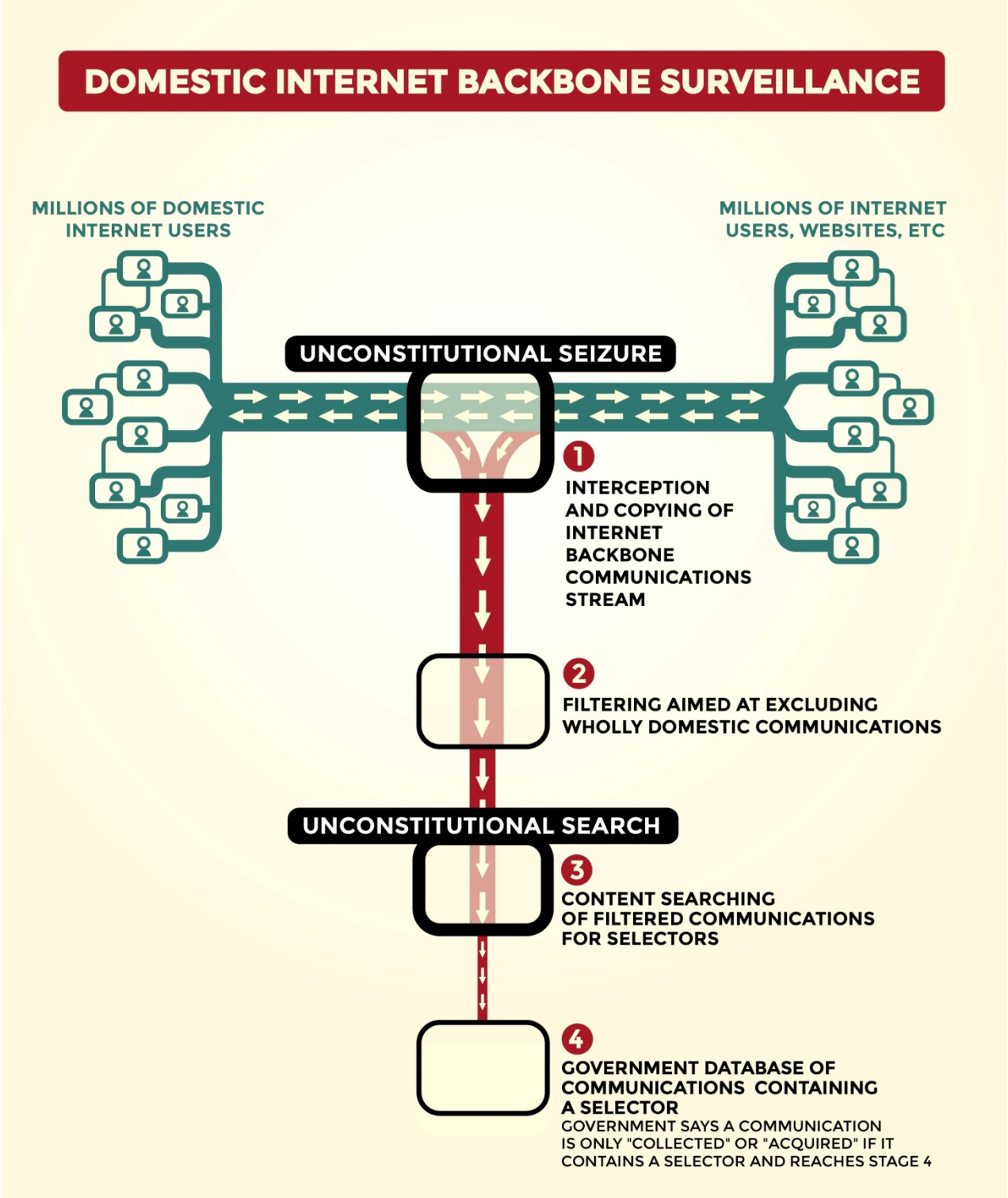
> transactions [plaintiffs' stage one] are first filtered to eliminate potential domestic transactions [plaintiffs' stage two], and then are screened to capture only transactions containing a tasked selector [plaintiffs' stage three]. Unless transactions pass both these screens, they are not ingested into government databases [plaintiffs' stage four].[9]

As the PCLOB notes, "[n]othing comparable [to the government's Internet backbone surveillance] is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication."[10]

[9] ER 125-26.

[10] ER 129.

The four stages of the government's surveillance process are illustrated below:



At stage one, the communications transiting the domestic Internet backbone are intercepted.[11] 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.[12]

At stage two, after the communications stream is copied, it is 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.[13] This filtering intentionally retains communications between Americans and persons located abroad. 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.[14]

---

[11] ER 120, 124-26, 59, 61, 105 (PCLOB Report); *see also* note 5 above.

[12] ER 257-58 (Klein Decl.) at ¶¶ 21-34; ER 364-487 (Klein Decl., Exs. A, B, C); ER 227-33, 240-41 (Marcus Decl.) at ¶¶ 56-58, 62, 70-73, 77, 109; ER 345-46, 348-52 (Russell Decl.) at ¶¶ 6, 10-12, 15, 19-23.

[13] ER 126, 58, 61 (PCLOB Report).

[14] One reason why the government's filtering fails to exclude domestic communications is the inaccuracy of Internet Protocol ("IP") filters it uses. ER 58 (PCLOB Report); ER 241 (Marcus Decl.) at ¶¶ 110-11. Another reason is that a communication between two domestic parties can follow a path that takes it outside the United States for part of its journey. The pathway a communication takes on the Internet from its origin to its destination is unpredictable and can change with every transmission; thus, "wholly domestic communications that are routed via a foreign server for any reason are susceptible to . . . acquisition if the [communication] contains

(footnote continued on following page)

At stage three, the *entire contents* of the filtered communications stream are searched for particular "selectors"—email addresses, domain names, phone numbers, or other identifiers.[15] The government refers to communications whose contents contain a reference to a selector, as opposed

---

(footnote continued from previous page)
a . . . selector." ER 61 (PCLOB Report). "[W]holly domestic communications also may be embedded within Internet transactions [i.e., groups of communications] that also contain foreign communications." *Id*. 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. ER 152 (President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*). In addition, providers of domestic Internet services may back up or store a user's data on servers anywhere in the world. For example, Yahoo! provides the AT&T-branded email services that plaintiffs Knutzen and Walton use. ER 110 (Knutzen Decl.) at ¶ 5; ER 107 (Walton Decl.) at ¶ 5. The NSA has intercepted massive bulk shipments of user email accounts by Yahoo! between its United States and overseas servers, shipments that are completely unknown to the user. ER 139-40 (Special Source Operations Weekly, 3/14/13 edition).

[15] "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 126 (PCLOB Report).

See also ER 120, 76, 59, 128-29 (PCLOB Report); ECF No. 227 at ¶ 64, p. 45:6-9 (12/23/13 NSA Deputy Dir. Fleisch Classified Decl.); ECF No. 254-1 at 8 (Corrected Government Defendants' Reply Brief Regarding Compliance With Preservation Orders; "'NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it'"); ER 233-35 (Marcus Decl.) at ¶¶ 82-85; ER 352 (Russell Decl.) at ¶ 23.

to being to or from a selector, as "about" communications.[16] As the PCLOB Report explains, "[d]igital 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."[17] The filtered communications that are searched include the international Internet communications of plaintiffs and other Americans, as well as many wholly domestic Internet communications as previously noted.

At stage four, the results of the seizing and searching described above are deposited into government databases for retention.[18] The communications the government retains at stage four are not at issue here.

Plaintiffs' Internet provider AT&T is one of the Internet backbone providers whose communications the government intercepts and searches.[19]

---

[16] ER 120, 126, 128-29 (PCLOB Report).

[17] ER 129 (PCLOB Report).

[18] ER 126, 127 n.476 (PCLOB Report).

[19] The declarations of former AT&T employee Mark Klein and of expert Scott Marcus, former Senior Advisor for Internet Technology to the Federal Communications Commission, demonstrate the NSA's interception, copying, and searching of plaintiffs' AT&T Internet communications from the Internet backbone. ER 254-56, 259 (Klein Decl.) at ¶¶ 8-10, 12, 14, 16-18, 36; ER 216-17, 225-36, 245-49 (Marcus Decl.) at ¶¶ 6, 44-49, 56-58, 62, 70-73, 77-90, 128-39, 146-47. Klein describes his personal observations of the government's Internet surveillance activities and provides AT&T documents relating to the government's surveillance activities.

The declaration of AT&T's Managing Director-Asset Protection James Russell authenticates the AT&T documents and confirms statements made

(footnote continued on following page)

Plaintiffs' summary judgment motion challenges the constitutionality of *stage one*, the wholesale seizure of the stream of Internet communications, and *stage three*, the searching of the filtered communications for selectors.

PROCEDURAL HISTORY

Plaintiffs filed their class action complaint on September 18, 2008. ER 284 (Complaint). The defendants include the United States, the National Security Agency, the Department of Justice, and official-capacity defendants Barack H. Obama, Michael S. Rogers, Loretta E. Lynch, and James R. Clapper, Jr. ("the government defendants"). To date, the district court has forbidden any discovery. ER 191.

(footnote continued from previous page)
by Klein and Marcus. ER 345-46, 349-52 (Russell Decl.) at ¶¶ 5-6, 15, 19-23.

Further evidence of AT&T's participation are the transparency reports AT&T issues confirming its participation in FISA surveillance. ER 79-83; *see also* ER 184-90.

The draft NSA Office of Inspector General Report also demonstrates AT&T's participation. ER 197-204 (draft NSA OIG Report). It describes how since 2001 the NSA has intercepted Internet communications "transiting the United States through fiber-optic cables, gateway switches, and data networks" of two telecommunications companies described as "Company A" and "Company B." ER 200-204. Company A and Company B were the two largest United States providers of international telephone calls when surveillance began in 2001. ER 201. Federal Communications Commission records confirm that AT&T was one of the two largest international telephone call providers at that time. ER 148-49 (FCC Common Carrier Bureau, 1999 International Telecommunications Data at 29, fig. 9 (Dec. 2000)).

In 2010, the district court *sua sponte* dismissed plaintiffs' action for lack of standing. ECF No. 57. In 2011, this Court reversed the dismissal. *Jewel v. NSA*, 673 F.3d 902, 905 (9th Cir. 2011). It found that plaintiffs "have standing to bring their statutory and constitutional claims against the government for what they describe as a communications dragnet of ordinary American citizens" "[i]n light of detailed allegations and claims of harm linking [plaintiffs] to the intercepted telephone, internet and electronic communications." *Id*.

On remand, plaintiffs moved for partial summary judgment on the issue of whether 50 U.S.C. § 1806(f) displaces the state secrets privilege; the government defendants 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. The district court held that section 1806(f) displaces the state secrets privilege, held that 18 U.S.C. § 2712 waived sovereign immunity for some of plaintiffs' statutory claims, and dismissed other statutory claims on sovereign immunity grounds. ER 15-40 (7/23/13 Amended Order).

Plaintiffs thereafter moved for partial summary judgment on their Fourth Amendment Internet interception claim. ECF Nos. 261, 294-3. The government defendants cross-moved for partial summary judgment on the same claim, contending that plaintiffs lacked evidence of standing, that even if plaintiffs had standing their Fourth Amendment claim failed on the merits,

and that alternatively the state secrets privilege barred litigation of plaintiffs' claim. ECF Nos. 285, 286, 299-3.

The district court granted the government defendants' summary judgment motion and denied plaintiffs' summary judgment motion. ER 5-14 (2/10/15 Order).

ISSUES

1. Have plaintiffs established their standing to challenge stage one by showing the copying of at least some of their Internet communications?

2. Have plaintiffs established their standing to challenge stage three by showing the searching of at least some of their Internet communications?

3. Are plaintiffs entitled to summary judgment on their claim that the stage-one copying of their Internet communications violates the Fourth Amendment?

4. Are plaintiffs entitled to summary judgment on their claim that the stage-three searching of their Internet communications violates the Fourth Amendment?

5. Does section 1806(f) of title 50 U.S.C. displace the state secrets privilege with respect to any secret evidence relevant to plaintiffs' Fourth Amendment claim?

ARGUMENT

I. Standard And Scope Of Review

This Court reviews de novo an order granting summary judgment and denying an opposing cross-motion for summary judgment, asking whether the evidence establishes a genuine dispute as to a material fact and whether the law entitles the movant to judgment. *Crowley v. Nevada ex rel. Nevada Secretary of State*, 678 F.3d 730, 733-34 (9th Cir. 2012); Fed. R. Civ. Pro. 56(a); *see also Jewel*, 673 F.3d at 907 ("standing . . . [is] a question of law that we review de novo").

For each motion, the Court views the evidence and draws all inferences in the light most favorable to the nonmoving party. *Bravo v. City of Santa Maria*, 665 F.3d 1076, 1083 (9th Cir. 2011); *A.C.L.U. of Nevada v. Las Vegas*, 466 F.3d 784, 790-91 (9th Cir. 2006). Assessing whether the nonmoving party has produced sufficient evidence to avoid summary judgment is done in light of the burden of proof. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986) ("whether reasonable jurors could find by a preponderance of the evidence that the plaintiff is entitled to a verdict").

II. Plaintiffs' Undisputed Evidence Establishes Their Standing

Standing is a threshold jurisdictional question that "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 Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir. 2011). Indeed, in the previous appeal in this case, the 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.

To establish their standing, plaintiffs need only show "(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; *accord Susan B. Anthony List v. Driehaus*, __ U.S. __, 134 S.Ct. 2334, 2341 (2014).

Standing is determined by the facts existing at the time the lawsuit was filed in 2008. *Davis v. Federal Election Commission*, 554 U.S. 724, 734 (2008); *A.C.L.U. of Nevada v. Lomax*, 471 F.3d 1010, 1015 (9th Cir. 2006).

The parties agreed that the merits of their summary judgment motions must be decided solely on the public evidence and that it would be improper to consider any of the government's secret evidence. 12/19/14 Reporter's Transcript at 25-27, 42-45, 47; ECF No. 285 at 54-55; ECF No. 294-3 at 32-34; ECF No. 299-3 at 17 n.18, 20. The government's position is a basic consequence of its invocation of the state secrets privilege, under which secret evidence is excluded from the case and not considered in deciding the merits. *Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007).

On the standing issue, the government defendants did not present any evidence attempting to prove that plaintiffs' communications were not intercepted, copied, and searched; they also did not introduce evidence disproving or undermining the evidence on which plaintiffs relied. Instead,

they argued that plaintiffs "cannot produce admissible evidence to support" standing. Fed. R. Civ. Pro. 56(c)(1)(B); *see* ECF No. 285 at 13.

Thus, if a reasonable factfinder could find it more probable than not that plaintiffs' communications have been copied and searched, the judgment for the government defendants on the issue of standing must be reversed. And, in that case, plaintiffs are entitled to judgment in their favor on standing: Because there is no evidence disputing plaintiffs' evidence showing that their communications have been copied and searched, there is no genuine dispute as to the facts material to standing.

A. Plaintiffs Have Demonstrated Their Standing To Challenge *Stage One* By Showing That At Least Some Of Their Communications Are Copied

Plaintiffs' evidence demonstrates that at least some of their Internet communications are copied, which is all that plaintiffs need show to establish an injury and give them standing for their Fourth Amendment challenge to stage one.

The government admits the following: The NSA intercepts and "acquire[s] communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the 'Internet backbone.'" ER 125-26 (PCLOB Report); *see also* ER 120, 124-26, 58-61 (PCLOB Report); ECF No. 227 at ¶ 38, p. 25:14-16. "[T]he [NSA] intercepts communications directly from the Internet 'backbone'" using

"NSA-designed . . . Internet collection devices [that] acquire transactions[20] [i.e., communications] as they cross the Internet." ER 105, 59 (PCLOB Report).

"[T]he acquisition occurs with the compelled assistance of providers that control the telecommunications 'backbone' over which . . . Internet communications transit." ER 120 (PCLOB Report); *see also* ER 124 (PCLOB Report). "The provider is compelled to assist the government in acquiring communications across these circuits."[21] ER 126 (PCLOB Report). The NSA's Internet backbone surveillance has continued since 2001. ER 50, 52-56 (PCLOB Report).

The NSA's surveillance begins with the entire stream of communications transiting the Internet backbone. By beginning at stage one with the full stream of "Internet transactions . . . on the Internet backbone" ER 126 (PCLOB Report), the selector-searching at stage three yields those communications transiting the Internet backbone that contain the chosen selectors. *See* ER 120, 76, 125-26 ("[S]electors used for the acquisition of upstream Internet transactions are sent to a United States electronic

[20] A "transaction" is a single communication or a group of communications. *See* n.8 above.

[21] Whether the seizures and searches here are conducted by the government directly or by AT&T at the government's direction is irrelevant. The Fourth Amendment applies whenever a "private party acts as an 'instrument or agent' of the government." *U.S. v. Young*, 153 F.3d 1079, 1080 (9th Cir. 1998).

communication service provider to acquire communications that are transiting through . . . the 'Internet backbone.'"), 61 (PCLOB Report).

The government admits that its interceptions occur "in the flow of communications between communication service providers." ER 124 (PCLOB Report). AT&T is a major provider of Internet services and one of the largest Internet backbone network operators.[22] AT&T's Internet facilities in San Francisco include interconnections between AT&T's Internet backbone and the Internet backbones of other Internet providers.[23]

All of the communications flowing across those interconnections between AT&T's Internet backbone network and the Internet backbones of other communications providers are copied using fiber-optic splitters.[24] The entire stream of communications copied by the splitters is then transmitted to a secure room in AT&T's facilities under the control of the NSA.[25] Plaintiffs are California residents who use AT&T's Internet services.[26] The

[22] ER 244 (Marcus Decl.) at ¶ 122.

[23] ER 256-58 (Klein Decl.) at ¶¶ 19, 22, 29-34; ER 345, 348-52 (Russell Decl.) at ¶¶ 6, 10, 15, 19, 21, 23.

[24] ER 257-59 (Klein Decl.) at ¶¶ 21-34, 36; ER 364-487 (Klein Decl., Exs. A, B, C); ER 227-32, 240-43 (Marcus Decl.) at ¶¶ 56-58, 62, 70-73, 77, 109, 113-18; ER 345, 348-52 (Russell Decl.) at ¶¶ 6, 10-12, 15, 19-23. *See also* ER 79-83, 148-49, 200-204.

[25] ER 254-56, 259 (Klein Decl.) at ¶¶ 8-10, 12, 14, 16-18, 36; ER 216-17, 225-26, 232, 234, 236, 245-49 (Marcus Decl.) at ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47.

[26] ER 113 (Jewel Decl.) at ¶¶ 1-5; ER 110 (Knutzen Decl.) at ¶¶ 1-6; ER 107 (Walton Decl.) at ¶¶ 1-7.

AT&T Internet backbone circuits that are copied carry the communications of plaintiffs and other AT&T customers.[27]

The government defendants put in no public evidence contesting these facts—and, as noted above, the parties agreed that the district court could consider only the public evidence in deciding whether plaintiffs have standing.

The government defendants' motion for summary judgment on plaintiffs' stage-one standing fails because a rational factfinder could easily conclude that it is more probable than not that plaintiffs' Internet communications have been intercepted and copied. Further, plaintiffs are entitled to summary judgment on the issue of standing to challenge stage one because the government defendants submitted no evidence creating a genuine dispute over any of the facts plaintiffs rely on to show the interception and copying of their communications.

B. Plaintiffs Have Demonstrated Their Standing To Challenge *Stage Three* By Showing That At Least Some Of Their Communications Are Searched

Plaintiffs' evidence demonstrates that at least some of their Internet communications are international communications that are searched for the presence of selectors, which is all that plaintiffs need show to establish an injury and give them standing to challenge stage three.

---

[27] ER 240 (Marcus Decl.) at ¶ 108.

The copies of AT&T's Internet backbone communications, including plaintiffs' communications, made at stage one are next filtered in stage two, according to the government in an attempt to exclude wholly domestic communications: "Internet transactions . . . on the Internet backbone . . . are first filtered to eliminate potential domestic transactions." ER 126 (PCLOB Report). NSA uses "technical means, such as Internet protocol ('IP') filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States." ER 58, 61 (PCLOB Report).

Plaintiffs use the Internet to communicate overseas, including by engaging in email correspondences with individuals in such countries as Saudi Arabia, Indonesia, England, Germany, Denmark, France, Canada, and Australia, as well as visiting foreign websites.[28] These international communications of plaintiffs thus pass through the stage-two filters to stage three.

At stage three, using selectors, the filtered communications of plaintiffs "are screened to capture only transactions containing a tasked selector." ER 126 (PCLOB Report); *see* ER 120, 76, 125-26 (PCLOB Report). The stage-three screening searches the contents of plaintiffs' communications looking for "the selector in the body of the

[28] ER 113-14 (Jewel Decl.) at ¶¶ 6-8; ER 110-11 (Knutzen Decl.) at ¶¶ 8-9; ER 107-108 (Walton Decl.) at ¶¶ 8-9.

communication." ER 120 (PCLOB Report); *see* ER 126, 128-29 (PCLOB Report).

The NSA performs its interception and searching of Internet backbone communications with the assistance of electronic communications service providers like AT&T who control Internet backbone facilities. ER 120, 76, 124-26, 58-61, 105 (PCLOB Report). The process of searching involves the NSA sending the selectors to the communications provider where they are used in NSA-designed devices that search the filtered Internet backbone communications. ER 120, 76, 125-26, 59, 61 (PCLOB Report). The AT&T secure room contains equipment designed to perform the filtering and searching of Internet communications, including searching the contents of electronic communications for selectors or other search terms and means for receiving the transmission of search terms from outside the room.[29] The NSA controls the operation of the AT&T secure room.[30]

Thus, the international communications of plaintiffs copied at stage one pass through the domestic communications filter at stage two and are searched for selectors at stage three. The government did not put in any

[29] ER 258-59 (Klein Decl.) at ¶¶ 28, 35; ER 429-87 (Klein Decl., Ex. C); ER 345-46, 349-52 (Russell Decl.) at ¶¶ 6, 15, 19, 22-23; ER 230-35 (Marcus Decl.) at ¶¶ 68, 70-77, 79-85.

[30] ER 254-56, 259 (Klein Decl.) at ¶¶ 8-10, 12, 14, 16-18, 36; ER 216-17, 225-26, 232, 234, 236, 245-49 (Marcus Decl.) at ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47.

evidence in the public record attempting to prove that none of plaintiffs' communications has been searched for selectors.

Plaintiffs' unrebutted evidence is sufficient not just to defeat summary judgment against them but to require summary judgment in their favor. A rational factfinder could easily conclude that it is more probable than not that at least some of plaintiffs' international Internet communications have been searched for selectors, defeating the government defendants' motion for summary judgment on plaintiffs' stage-three standing. And because the government defendants submitted no evidence creating a genuine dispute over any of the facts plaintiffs rely on to show the searching of their communications, plaintiffs are entitled to summary judgment on the issue of standing to challenge stage three.

C. The District Court Erred In Granting Summary Judgment On The Ground That Plaintiffs Lacked Standing

1. The District Court Misunderstood What Plaintiffs Must Show To Establish Standing

The district court erred in granting summary judgment in favor of the government defendants on the ground that plaintiffs had no evidence from which a rational factfinder could conclude they had suffered any injury. ER 8-12.

The district court misunderstood both plaintiffs' contentions and their burden in establishing standing: it erroneously described plaintiffs as contending that "all of their Internet communications have been collected

and amassed in storage." ER 10. Plaintiffs' motion, however, makes no contention that all, or even any, of their communications are ultimately stored by the government at stage four; nor do plaintiffs contend that all of their communications are copied at stage one or searched at stage three. For standing to challenge stage one and stage three, all plaintiffs need show, as they have by the undisputed public evidence, is that at least one or more of their international Internet communications have been copied and searched.

The district court also erred when it weighed the government's secret evidence against plaintiffs' public evidence and concluded "Plaintiffs' version . . . is substantially inaccurate." ER 12. It violated both the rule that a court may not weigh the evidence on summary judgment and the rule that evidence excluded under the state secrets privilege may not be considered on the merits. *Al-Haramain*, 507 F.3d at 1204.

More fundamentally, what matters for standing is not whether all of plaintiffs' inferences from the public evidence correspond with the government's secret version of the facts, but whether the public evidence supports those few facts that are material to plaintiffs' standing: for stage one, the copying of at least some of plaintiffs' Internet communications, and, for stage three, the searching of at least some of plaintiffs' international communications for selectors. In particular, given the government's admission that it intercepts the mixed domestic and international communications traffic transiting the Internet backbone and searches the international communications within that traffic for selectors, there is no

plausible basis for believing that the government has not copied and searched at least one international communication from each plaintiff, and it is impossible that no member of the class has had their communications copied and searched.

2. The District Court Improperly Disregarded Plaintiffs' Undisputed Evidence

The district court improperly failed to view the evidence in the light most favorable to plaintiffs and give it the full weight it deserved.

The court discounted the testimony of Klein, Marcus, and Russell and ignored the AT&T documents, erroneously concluding that "Klein cannot establish the content, function, or purpose of the secure room" or "what data were actually processed and by whom in the secure room." ER 12. The district court's conclusion is mistaken, as is its premise that plaintiffs must prove their standing using Klein's evidence alone (especially given the government's extensive admissions).

As an initial matter, the PCLOB Report is clear that "[t]he provider is compelled to assist the government in acquiring communications across these [Internet backbone] circuits." ER 126 (PCLOB Report). So there is no dispute that providers like AT&T are involved in the acquisition of communications over the Internet backbone.

The district court ignored that the Klein and Marcus evidence is corroborated by the government's admissions. Those admissions describe a process that begins with "intercept[ing] communications directly from the

Internet 'backbone'" with the compelled assistance of Internet backbone providers, followed by content searching of communications—the same process described by Klein and Marcus. ER 105, 126, 58 (PCLOB Report).

Evidence Regarding The Communications That Were Copied And Processed:

Klein's testimony is solidly grounded in his own personal knowledge, based on his decades of experience with AT&T's business practices and operations and his observations and activities in the course of his employment. *Barthelemy v. Air Lines Pilots Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990) ("personal knowledge and competence to testify are reasonably inferred from [employees'] positions and the nature of their participation in the matters to which they swore").

Klein has personal knowledge of what was copied by the splitters and "what data were actually processed . . . in the secure room" (ER 12) because he was in charge of copying AT&T's Internet backbone communications and transmitting the copies to the AT&T secure room over fiber-optic cables.[31] As directed by the AT&T documents he relied upon to do his job, he physically connected the Internet backbone circuits to the splitters he operated, and he describes in detail the circuits connected to the splitters and the types of data they carry.[32]

[31] ER 255-58 (Klein Decl.) at ¶¶ 15, 27, 34.

[32] ER 256-59 (Klein Decl.) at ¶¶ 19, 22, 25, 26, 28-34, 36; ER 364-487 (Klein Decl., Exs. A, B, C).

AT&T's Russell independently verifies this information, as do the AT&T documents.[33] The AT&T documents are admissible both as AT&T business records[34] and as statements by AT&T as the government's agent. Fed. R. Evid. 801(d)(2)(D), 803(6).

Evidence Regarding The Search Devices In The AT&T Secure Room:

Klein's testimony regarding the electronic search devices inside the AT&T secure room that were attached to the other end of the fiber-optic cables he was responsible for maintaining is based on the AT&T documents he relied upon in his job.[35] AT&T's Russell testifies that the devices described by Klein and listed in the AT&T documents actually are present in the secure room.[36] Russell also testifies that the search devices in the secure room that Marcus analyzes are present there.[37]

Evidence Regarding The NSA's Involvement:

Nor is there any doubt that the copying and searching of plaintiffs' communications is occurring at the government's direction. (Again, the

[33] ER 349-51 (Russell Decl.) at ¶¶ 15, 19, 21; ER 364-487 (Klein Decl., Exs. A, B, C).

[34] *See* ER 257-58 (Klein Decl.) at ¶¶ 25-26, 28; ER 345-46, 351-52 (Russell Decl.) at ¶¶ 5-6, 20-22.

[35] ER 258-59 (Klein Decl.) at ¶¶ 28, 35; ER 429-87 (Klein Decl., Ex. C).

[36] ER 345-46, 349-52 (Russell Decl.) at ¶¶ 6, 15, 19, 22.

[37] ER 352 (Russell Decl.) at ¶ 23; *see* ER 230-35 (Marcus Decl.) at ¶¶ 68, 70-77, 79-85.

PCLOB Report is clear about the government's direction of providers.) Klein's testimony of the NSA's involvement in the AT&T secure room at his workplace is based on his personal observations and experiences on the job. It is no different than any other testimony by an employee regarding his on-the-job experiences, his observations of co-workers, his company's policies and practices, or its interactions with another entity.

Employees may testify about the functions and activities of others within the organization that employs them and about the relationship between the organization and outside entities, including government entities. *U.S. v. Neal*, 36 F.3d 1190, 1206 (1st Cir. 1994); *Great American Assur. Co. v. Liberty Surplus Ins. Corp.*, 669 F.Supp.2d 1084, 1089 (N.D. Cal. 2009) (employee can testify to company policies based on her "experience and perceptions" on the job); *Sjoblom v. Charter Communications, LLC*, 571 F.Supp.2d 961, 968-69 (W.D. Wis. 2008) (employees may testify about the activities of their supervisors and co-workers that they observe).[38]

[38] *Accord U.S. v. Famania-Roche*, 537 F.3d 71, 76 (1st Cir. 2008) (low-level drug dealer could testify to activities and drug sales by other drug dealers in narcotics organization she was part of); *DIRECTV, Inc. v. Budden*, 420 F.3d 521, 529 (5th Cir. 2005) (employee could testify about facts concerning another company he learned through a law enforcement investigation); *U.S. v. Doe*, 960 F.2d 221, 223 (1st Cir. 1992) (gun shop owner could testify that pistol sold to him by another United States company was manufactured in Brazil); *White v. MPW Indus. Servs., Inc.*, 236 F.R.D. 363, 369 (E.D. Tenn. 2006) ("employees . . . would have learned during the normal course of their employment how the company operates and what the company's policies were"); *U.S. v. Wirtz*, 357 F.Supp.2d 1164, 1169-70 (D. Minn. 2005) (employee could testify that employees of a different company provided

(footnote continued on following page)

Moreover, an employee's "[p]ersonal knowledge can include 'inferences and opinions, so long as they are grounded in personal observation and experience.'" *Neal*, 36 F.3d at 1206; *see also* Fed. R. Evid. 701 (lay opinion).

For instance, in *Neal*, a bank employee testified to information she learned in the course of her job, including the status of the bank's relationship with a federal agency (the Federal Deposit Insurance Corporation) and the states where the bank's customers were located, even though her knowledge was based solely on hearsay statements in documents she reviewed. 36 F.3d at 1206.

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 from only the secure room is because AT&T's policy was to restrict access to only persons cleared by the NSA, even in emergencies.[39] Likewise, Klein testified from his personal knowledge about visiting the secure room while it was under construction (where he saw AT&T employee "FSS #2," whom Klein had observed meeting with an NSA agent and whom Klein knew to be in charge of the room, installing equipment) and of again

---

(footnote continued from previous page)
certain information and documents to his company even though he had no personal contact with the employees of the other company).

[39] ER 256 (Klein Decl.) at ¶¶ 17, 18.

visiting the secure room after it was in operation.[40] And Klein's statements that "The NSA agent came and met with FSS #2" and "The NSA agent did come and speak to [AT&T employee] FSS #1" are also personal observations.[41]

The statements made to Klein by AT&T management and co-workers about the NSA's activities and the secure room are admissible nonhearsay. AT&T is the agent of the government in assisting the government in electronic surveillance, and statements by an agent on a matter within the scope of the agency are admissible nonhearsay. Fed. R. Evid. 801(d)(2)(D).

The e-mail to Klein from AT&T management and statements by his manager and a co-worker telling of upcoming visits by an NSA agent are independently admissible under Federal Rule of Evidence 803(3) as evidence that AT&T employees actually met with NSA agents, that the purpose of the first meeting was that "the NSA agent was to interview FSS #2 for a special job" and that the purpose of the second meeting was to discuss "FSS #3's suitability to perform the special job that FSS #2 had been doing," that AT&T's management's plan and intent was to cooperate with the NSA, and that AT&T thereafter did cooperate with the NSA.[42] Fed. R. Evid. 803(3) (statements reflecting plan or intent are admissible); *U.S. v.*

[40] ER 255-56 (Klein Decl.) at ¶¶ 10, 12, 14, 17.

[41] ER 255-56 (Klein Decl.) at ¶¶ 10, 16.

[42] ER 255-56 (Klein Decl.) at ¶¶ 10, 16.

Best, 219 F.3d 192, 198 (2d Cir. 2000) (statement of plan or intent can be used to "prove that the declarant thereafter acted in accordance with the stated intent"); *U.S. v. Donley*, 878 F.2d 735, 737-38 (3d Cir. 1989) (same); *U.S. v. Astorga-Torres*, 682 F.2d 1331, 1335 (9th Cir. 1982) (same).

Marcus's Expert Testimony:

The district court also improperly discounted Marcus's expert testimony, mistakenly believing that "Marcus relies exclusively on the observations and assumptions by Klein." ER 12. Marcus's testimony, however, is based not just on Klein's testimony, but also on the AT&T documents and other independent evidence Marcus cites and on Marcus's decades of knowledge and personal experience in the telecommunications field, including providing Internet backbone services to AT&T.[43] Marcus independently concluded that government surveillance is the purpose of the equipment Klein describes, without relying on any of Klein's statements regarding the NSA's participation and without relying on any "assumed operational details" (ER 12).[44] Marcus's testimony about the "purpose and function of the secure equipment at AT&T" (ER 12) is based on the AT&T documents showing the existence of that equipment in the AT&T secure

[43] ER 217-21 (Marcus Decl.) at ¶¶ 7, 13-18, 24, 27, 29.

[44] ER 216-17, 225-26, 232, 234, 236, 245-49 (Marcus Decl.) at ¶¶ 6, 44-49, 75, 83, 88, 128-39, 146-47.

room (a fact confirmed by Russell) and on his independent expert knowledge about the capabilities of that equipment.[45]

3. The District Court Erred In Granting Summary Judgment Without Permitting Discovery

The district court's grant of summary judgment was erroneous for the additional, independent reason that it barred plaintiffs from conducting any discovery. A district court cannot grant summary judgment to a defendant until it has provided "adequate time for discovery" to the plaintiff. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Since the outset of this lawsuit, the district court has barred plaintiffs from conducting any discovery. *See* Fed. R. Civ. Pro. 56(d); ER 191, 205-10, 278-83; 9/27/13 Reporter's Transcript at 8, 12-13; ECF No. 294-3 at 35.

III. Plaintiffs Are Entitled To Summary Judgment On The Merits Of Their Fourth Amendment Claim

A. The Fourth Amendment Protect Plaintiffs' Internet Communications From Suspicionless, Indiscriminate Searches And Seizures

1. The Fourth Amendment Protects Plaintiffs' Internet Communications

The Fourth Amendment is a fundamental guarantee of personal privacy "which 'is basic to a free society.'" *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 528 (1967). "The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals

[45] ER 230-35 (Marcus Decl.) at ¶¶ 67-68, 70-77, 79-85.

against arbitrary invasions by governmental officials." *Id*. 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).

Protecting privacy in personal communications like plaintiffs' Internet communications is one of the core principles of the Fourth Amendment. The Fourth Amendment 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. __, 132 S.Ct. 945, 950 (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. *Riley v. California*, 573 U.S. __, 134 S.Ct. 2473, 2494 (2014); *Stanford v. Texas*, 379 U.S. 476, 480-85 (1965); *Marcus v. Search Warrants of Property*, 367 U.S. 717, 726-29 & n.22 (1961).

The Fourth Amendment 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." *U.S. v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). 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. These records are expected to be kept private and this expectation is one that society is prepared to recognize as reasonable." *Id*. at 964 (citations and internal quotation marks omitted); *accord U.S. v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).

The Fourth Amendment also 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).

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.[46] *Berger v. New York*, 388 U.S. 41, 51 (1967); *Cotterman*, 709 F.3d at 964;

[46] The "reasonable expectation of privacy test" is the alternative test for the scope of Fourth Amendment protections. *See Jones*, 132 S.Ct. at 950, 953; *id*. at 954-55 (Sotomayor, J., concurring); *id*. at 959-60 (Alito, J., concurring).

see also U.S. v. U.S. District Court (Keith), 407 U.S. 297, 313 (1972) (hereinafter, "*Keith*"); *Katz v. U.S.*, 389 U.S. 347, 353 (1967).

The Supreme Court recently affirmed that the government's search and seizure of digital information implicates core Fourth Amendment values and triggers the warrant requirement. *Riley*, 134 S.Ct. at 2495 ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."). The Court specifically noted the protected privacy interests in Internet browsing: "Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD." *Id*. at 2490. The Court went on to detail how a person's digital information because of its breadth and depth 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 2489-91.

The Fourth Amendment privacy interests in digital information that the Supreme Court recognized in *Riley* are fully applicable to the Internet activities of plaintiffs that the government is seizing and searching—including emails, web browsing and searching, live chat, voice calls, social networking, photos, and videos—because of "all they contain and all they may reveal." *Riley*, 134 S.Ct. at 2494-95. Indeed, the Court noted that much of the digital information it protected in *Riley* is increasingly not stored on smartphones themselves but in the Internet "cloud," with phones

used to access the information over the Internet. *Id*. at 2491. Because communications between smartphones and the Internet "cloud" often transit the Internet backbone, those communications are subject to the NSA's interception.

2. The Warrant Requirement Applies To The Seizure And Searching Of Plaintiffs' Internet Communications

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 communications to be seized. *See Ex parte Jackson*, 96 U.S. at 733. National security does not excuse the need for a warrant to intercept or search plaintiffs' communications. "It is now clear that [the warrant] requirement attaches to national security wiretaps that are not directed against foreign powers or suspected agents of foreign powers." *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986) (Scalia, Circuit Justice, for the court).

The warrant requirement is not a dusty formalism but *the* 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*, 134 S.Ct. at 2493 (internal quotation marks omitted).

The probable cause requirement ensures that no search 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 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. It 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. "Search warrants . . . are fundamentally offensive to the underlying principles of the Fourth Amendment when they are so bountiful and expansive in their language that they constitute 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).

Judicial warrants founded on particularity and probable cause are crucial in electronic surveillance because those searches and seizures occur without leaving a trace. *Keith*, 407 U.S. at 313, 318; *Berger*, 388 U.S. at 63. 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.

B. Stage One: The Government's Warrantless, Suspicionless Mass Copying Of Internet Communications Is A Seizure That Violates The Fourth Amendment

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—is an unconstitutional seizure. It is a suspicionless general seizure that is not, and never could be, authorized by a valid warrant.

A seizure occurs when there is a meaningful interference with a possessory interest. *U.S. v. Jacobsen*, 406 U.S. 109, 113 (1984). The government concedes for purposes of these motions that plaintiffs have a possessory interest and a privacy interest in their Internet communications. 12/19/14 Reporter's Transcript at 75:19-24; *see U.S. v. Thomas*, 447 F.3d

1191, 1197-99 (9th Cir. 2006) ("[a] 'possessory or ownership interest' need not be defined narrowly"; unauthorized driver of a rental car had possessory interest in the car). The exercise of dominion and control by the government is one type of meaningful interference that results in a seizure. *Jacobsen*, 406 U.S. at 120-21 & n.18.

Here, 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).

No warrant could justify the mass, suspicionless seizures occurring here. "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), and its words "reflect the determination of those who wrote the Bill of Rights that the people of this new Nation should forever 'be secure in their persons, houses, papers, and effects' from intrusion and seizure by officers acting under the unbridled authority of a general warrant," *Stanford*, 379 U.S. at 481-82.

The government's indiscriminate, suspicionless bulk seizure of plaintiffs' Internet activities here is the modern-day equivalent of the hated

general warrants that the Fourth Amendment was meant to stamp out forever. 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.

C. Stage Three: The Government's Warrantless, Suspicionless Searching Of The Contents Of Plaintiffs' Internet Communications Violates The Fourth Amendment

The government's suspicionless and indiscriminate content searching of plaintiffs' Internet communications after it seizes them—stage three of the government's surveillance—is separately unconstitutional because it is conducted without a warrant, and because it is a general search that no warrant could properly authorize. If the Fourth Amendment means anything, it means that the government may not engage in indiscriminate, suspicionless, mass surveillance of its own citizens. Such surveillance "'alter[s] the relationship between citizen and government in a way that is inimical to a democratic society,'" *Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring), giving the government the power to peer into its citizens' private communications at any moment. That is exactly what the government has done here, in violation of the Fourth Amendment, by sitting on the Internet backbone and seizing and searching the communications of millions of Americans.

At stage three, the government searches for selectors the contents of the Internet activities of vast numbers of innocent Americans.[47] 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 with no connection to any surveillance target and about whom the government has no suspicions. This includes plaintiffs, none of whom is suspected of any wrongdoing but each of whom communicates with people abroad and visits websites hosted abroad.[48]

Because plaintiffs' communications fall within the Fourth Amendment's categorical protection of a person's "papers" and "effects," the warrantless searching of their communications is *per se* a Fourth Amendment violation. *See Florida v. Jardines*, __ U.S. __, 133 S.Ct. 1409, 1414 (2013) ("When the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original

[47] As previously noted, the government's filtering at stage two to exclude domestic communications is imperfect, and its stage-three searching includes domestic as well as international communications. *See* n.14 above.

[48] *See* ER 113-14 (Jewel Decl.) at ¶¶ 6, 8; ER 110-11 (Knutzen Decl.) at ¶¶ 8, 9; ER 107-108 (Walton Decl.) at ¶¶ 8, 9.

meaning of the Fourth Amendment has undoubtedly occurred." (internal quotation marks omitted)); *Jones*, 132 S.Ct. at 950 n.3 (same).

Independently, plaintiffs' reasonable expectation of privacy in their communications is violated when the government searches their communications without a warrant and without suspicion. *Katz*, 389 U.S. at 353, 356-59; *Berger*, 388 U.S. at 55-64; *Halperin*, 807 F.2d at 185.

The government's warrantless searching of the communications of persons not suspected of any wrongdoing 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). In the Fourth Amendment, the Founders "emphasize[d] the purpose to protect 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). "Opposition to such searches was in fact one of the driving forces behind the Revolution itself." *Riley*, 134 S.Ct. at 2494.

Like general warrants, searching the communications of millions of persons not under any suspicion is unconstitutional because it gives the government "the most general discretionary authority," *Marcus*, 367 U.S. at 726; has no limits on place or duration, *id*. at 729 n.22; and "provide[s] no judicial check on the determination of the executing officials that the

evidence available justifie[s] an intrusion," *Steagald v. U.S.*, 451 U.S. 204, 220 (1981).

D. The "Special Needs" Exception Cannot Justify The Government's Dragnet

"In most circumstances, searches and seizures conducted without a warrant are '*per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" *Al Haramain Islamic Foundation, Inc. v. U.S. Department of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011) (quoting *Katz*, 389 U.S. at 357). One of these exceptions to the warrant requirement is the "closely guarded" special needs exception. *Chandler v. Miller*, 520 U.S. 305, 309 (1997).

The government did not carry its burden of justifying under the special needs exception the warrantless, suspicionless mass seizures and searches of communications that plaintiffs challenge.[49] "When such 'special needs'—concerns other than crime detection—are alleged in justification of a Fourth Amendment intrusion, courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties." *Chandler*, 520 U.S. at 314 (internal citations omitted); *accord Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001).

[49] "The government bears the burden of demonstrating that an exception to the warrant requirement exists in any given case." *U.S. v. Fowlkes*, 770 F.3d 748, 756 (9th Cir. 2014).

Under the special needs inquiry, "'[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion.'" *Chandler*, 520 U.S. at 314 (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 624 (1989)); *accord Ferguson*, 532 U.S. at 78 ("a balancing test that weighed the intrusion on the individual's interest in privacy against the 'special needs' that supported the program").

The suspicionless mass search and seizure of Americans' Internet communications fails the first prong of the special needs exception, which requires that "'the privacy interests implicated by the search [be] minimal.'" *Chandler*, 520 U.S. at 314 (quoting *Skinner*, 489 U.S. at 624). Far from being "minimal," plaintiffs' privacy interests in their Internet activities and communications lie at the heart of the Fourth Amendment. A person's Internet activities reveal a vast array of intimate details about that person's private life. *See Riley*, 134 S.Ct. at 2489-91, 2494-95.

"The cases in which the [Supreme] Court has found warrantless searches to be reasonable all involve . . . greatly diminished privacy interests—a point repeatedly emphasized by the Court." *Al Haramain*, 686 F.3d at 994. Examples of special needs searches in which the person searched has a diminished expectation of privacy include students who voluntarily choose to participate in extracurricular activities, *see Board of*

Education of Indep. School Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 830-32 (2002); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 654-57 (1995), and workers who voluntarily choose employment in professions that put the safety of others at risk, *see Skinner*; *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 671-72 (1989). As Justice Kennedy has explained: "An essential, distinguishing feature of the special needs cases is that the person searched has consented, though the usual voluntariness analysis is altered because adverse consequences (*e.g.*, dismissal from employment or disqualification from playing on a high school sports team) will follow from refusal." *Ferguson*, 532 U.S. at 90-91 (Kennedy, J., concurring).

Here, plaintiffs have an *undiminished* expectation of privacy in the content of their electronic communications. They are not engaging in activities that diminish their expectations of privacy and have not otherwise consented to the search.

And the *intrusion* into plaintiffs' privacy interest in their communications is pervasive, not minimal. The government seizes the communications flowing through AT&T's Internet backbone connections and, after the stage-two filtering, searches the entire contents of millions of those communications, every word from top to bottom, to see whether they contain any selectors.

None of the Supreme Court's decisions approving special needs searches involved circumstances remotely similar to those present here.

None of those cases involved the suspicionless content-searching of papers or communications. None of those cases involved seizures and searches of the vast scale and magnitude occurring here, extending across the breadth of American society. Testing student athletes or train operators for drug use is nothing like searching the contents of the Internet communications of millions of ordinary Americans. Because there is a substantial intrusion on plaintiffs' undiminished expectations of privacy, the special needs exception does not apply.

Even if it were appropriate to proceed to balance the substantial intrusion on plaintiffs' privacy against the government's interest, the balance here weighs in favor of plaintiffs. The government's interest in acquiring foreign intelligence information, weighty as it is, does not give it a blank check to use any and every means of surveillance to pursue that interest regardless of how deep and widespread the intrusion into the privacy of innocent Americans. *Al Haramain*, 686 F.3d at 993 ("government's interest in preventing terrorism," while "extremely high," "is no excuse for dispensing altogether with domestic persons' constitutional rights"); *Home Building & Loan Ass'n v. Blaisdell*, 290 U.S. 398, 425-26 (1934) ("[E]ven the war power does not remove constitutional limitations safeguarding essential liberties.").

Additionally, the government must show that the primary purpose of the intrusion is something other than law enforcement. *City of Indianapolis v. Edmond*, 531 U.S. 32, 40-48 (2000).

The government failed to satisfy the primary-purpose test. Strikingly, it did not contend that the primary purpose of its Internet backbone surveillance is to collect foreign intelligence information. Instead, it asserted only that foreign intelligence collection is "a 'significant purpose'" of its Internet backbone surveillance. ECF No. 285 at 46-47 & n.10 (asserting only that it "serves the Government's need to obtain foreign intelligence" while also promoting other interests).

The government limits itself for a reason to claiming that foreign intelligence is no more than a significant purpose. The reason is that the government also retains any communications that contain evidence of a crime or information concerning an imminent threat of death or serious bodily harm, all of which are ordinary law enforcement concerns. ER 176-77, 179. Indeed, the FBI routinely searches communications collected by the NSA's Internet surveillance when investigating ordinary crimes. ER 130-31 (PCLOB Report).

Finally, the government must also show that complying with the warrant requirement would be impracticable. *Skinner*, 489 U.S. at 631. The government did not show it lacks other practicable alternatives to the mass suspicionless seizures and searches occurring here. The government argued that it would be inconvenient and time-consuming for it to comply with the warrant requirement (ER 70-71), but the Supreme Court in *Riley* rejected the view that the warrant requirement is an inconvenience to be weighed against claims of efficiency. *Riley*, 134 S.Ct. at 2493. The government may believe

that mass surveillance is a more convenient method of detecting wrongdoing or ferreting out information, but if the Fourth Amendment could be overcome by a showing of mere convenience alone, privacy would cease.

Moreover, *Riley* noted that "[r]ecent technological advances" have "made the process of obtaining a warrant itself more efficient," reducing the time required to as little as 15 minutes. *Riley*, 134 S.Ct. at 2493. The government's process for approving selector searches already requires that an NSA analyst document the grounds justifying the search and that two senior NSA analysts review and approve the search. ECF No. 285-1 at 6-7. The government does not explain why adding a neutral and detached magistrate to this process to ensure compliance with the Fourth Amendment's warrant requirement would be impossible.

Finally, as *Riley* noted, for truly exigent circumstances where there is insufficient time to obtain a warrant, the government can seek to avail itself of the exigent-circumstances exception to the warrant requirement. *Riley*, 134 S.Ct. at 2494.

IV. Section 1806(f) Displaces The State Secrets Privilege Here

A. Congress Has Displaced The State Secrets Privilege With Section 1806(f) In Lawsuits Involving Electronic Surveillance

The district court's alternative ground for summary judgment—the state secrets privilege—lacks merit because Congress had displaced the state secrets privilege with the procedures for using secret evidence set forth in

section 1806(f) of title 50 U.S.C. Section 1806(f), "unlike the common law state secrets privilege, provides a detailed regime to determine whether surveillance 'was lawfully authorized and conducted.'" *Al-Haramain*, 507 F.3d at 1205.

Congress recognized that in civil actions challenging unlawful electronic surveillance, the evidence may include sensitive national security information. In section 1806(f), Congress established a procedure enabling those actions to go forward to a decision on the legality of the surveillance while protecting the secrecy of that information. Rather than excluding national security evidence, as the state secrets privilege does, Congress instead displaced the privilege and directed courts to decide the legality of the surveillance, using relevant national security evidence, reviewed *in camera* and *ex parte* where necessary.

Section 1806(f) provides a method for the district court "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" in those instances where the government tells the court that "disclosure or an adversary hearing would harm the national security of the United States." § 1806(f). The district court is to make its merits determination by "review[ing] in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary,"

rather than excluding such evidence as would occur if the state secrets privilege were applied to it.[50] *Id.*

In cases involving electronic surveillance, section 1806(f) displaces and supersedes the common-law state secrets privilege. Congress expressly provided that section 1806(f) applies "notwithstanding any other law," thus confirming its intent to displace the state secrets privilege in cases challenging the lawfulness of electronic surveillance. § 1806(f); *see also* Fed. R. Evid. 501 (providing that privileges are displaced whenever a statute "provides otherwise").

Thus, if the government had wished to rely on national security evidence in the summary judgment proceedings, it was required to invoke section 1806(f). But section 1806(f) does not permit the government to artificially limit the record to a few cherry-picked facts in a handful of secret declarations. Instead, section 1806(f) contemplates that plaintiffs may propound discovery seeking "materials relating to electronic surveillance" for the district court's *ex parte*, *in camera* review. § 1806(f). In turn, the district court is to obtain and review *all* of the "materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted," rather than relying only on a selective record chosen by the government. *Id.*

[50] The full text of section 1806(f) is set forth in the statutory and constitutional addendum hereto.

B. FISA's Statutory Purpose And Legislative History Confirm That Section 1806(f) Displaces The State Secrets Privilege

The statutory purpose and legislative history of FISA, of which section 1806(f) is a part, further confirm section 1806(f)'s displacement of the state secrets privilege. FISA was enacted in 1978 in the wake of a Senate investigation—the "Church Committee"—revealing that for many decades the Executive, without any warrants or other lawful authority, had been conducting massive, secret dragnet surveillance invading the privacy and violating the Fourth Amendment rights of thousands of ordinary Americans. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, S. Rep. No. 94-755, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS ("BOOK II") at 139, 289-90 (1976).[51]

FISA was Congress' implementation of the Church Committee's call for "fundamental reform" "by enactment of a comprehensive legislative charter" that "cover[s] the field." BOOK II at 289, 297 & n.10, 336-37; S. Rep. No. 95-604(I) at 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. FISA implements the Committee's recommendations by imposing comprehensive limits on the Executive's power to conduct electronic surveillance and by creating civil remedies for unlawful surveillance.

[51] *Available at* http://www.intelligence.senate.gov/sites/default/files/94755_II.pdf.

To make judicial enforcement of the limitations on electronic surveillance possible, Congress created section 1806(f)'s requirement that courts use national security evidence to determine the legality of surveillance, instead of excluding that evidence under the state secrets privilege. The Church Committee anticipated section 1806(f) in stating that "courts will be able to fashion discovery procedures, including inspections of materials in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." BOOK II at 337. Section 1806(f) thus provides the practical means by which the substantive limitations on surveillance can be litigated without endangering national security.

C. Section 1806(f) Encompasses Civil Cases Arising Out Of Electronic Surveillance

FISA's legislative history confirms that section 1806(f) applies to civil cases, including constitutional claims. The House-Senate FISA conference committee adopted a single procedure for both criminal cases and civil cases in which a plaintiff is seeking a determination of the legality of electronic surveillance in order to vindicate constitutional and statutory rights:

> The conferees agree that an in camera and ex parte proceeding [i.e., section 1806(f)] is appropriate for determining the

> lawfulness of electronic surveillance in both criminal and civil cases.

H.R. Conf. Rep. No. 95-1720 at 32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061; *see also* H.R. Rep. No. 95-1283(I) at 93 (1978) ("A decision of illegality [of government surveillance] may not always arise in the context of suppression; rather it may, for example, arise incident to a discovery motion in a civil trial.").

Section 1806(f) applies equally to constitutional and statutory claims. Under it, a district court "determine[s] whether the surveillance was authorized and conducted in a manner which did not violate any *constitutional* or statutory right." S. Rep. No. 95-701 at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 (emphasis added); *accord* S. Rep. No. 95-604(I) at 57, 1978 U.S.C.C.A.N. at 3959. Congress' decision to create section 1806(f) as a means of litigating constitutional claims accords with "[t]he judiciary's essential role in protecting constitutional rights" and the fundamental principle that constitutional claims deserve a judicial forum. *In re National Security Agency Telecommunications Records Litigation*, 671 F.3d 881, 899 & n.3 (9th Cir. 2011). As this Court has held with respect to the very allegations at issue in this case, "[t]he federal courts remain a forum to consider the constitutionality of the wiretapping scheme." *Id*.

D. The District Court Erred In Failing To Apply Section 1806(f) Here

In the summary judgment proceedings, the district court without explanation failed to apply section 1806(f) to plaintiffs' Fourth Amendment

claim. By contrast, in earlier proceedings, the district court had correctly ruled that section 1806(f) displaced the state secrets privilege with respect to plaintiffs' statutory claims. ER 16, 26-29.

In those earlier proceedings, the district court held that section 1806(f)'s "*in camera* review procedure in FISA applies and preempts the determination of evidentiary preclusion under the state secrets doctrine. Section 1806(f) of FISA displaces the state secrets privilege in cases in which electronic surveillance yields potentially sensitive evidence by providing secure procedures under which courts can consider national security evidence that the application of the state secrets privilege would otherwise summarily exclude." ER 26. It thereby "permit[s] courts to determine whether any particular surveillance was lawfully authorized and executed." ER 27. Section 1806(f) "'occup[ies] the field'" and "leaves no room for application of the state secrets privilege." ER 28-29.

Thereafter, the government conceded that "the reasoning by which the Court concluded that section 1806(f) preempts application of the privilege to Plaintiffs' statutory claims would apply equally to Plaintiffs' constitutional claims." ECF No. 167 at 2, 14. Thus, it was undisputed that the district court's ruling that section 1806(f) displaces the state secrets privilege applied to plaintiffs' Fourth Amendment claim.

The government nonetheless again asserted the state secrets privilege on summary judgment. Plaintiffs opposed by again relying on section

1806(f), as well as explaining why the privilege has no application here even absent section 1806(f).

Unaccountably, without addressing plaintiffs' contentions or the impact of its prior section 1806(f) order, the district court held that the state secrets privilege applied to plaintiffs' Fourth Amendment claim and provided an alternative ground for dismissing plaintiffs' claim. ER 6, 12-13.

The district court's earlier holding that section 1806(f) occupies the field and displaces the state secrets privilege remains correct nonetheless. Its unexplained refusal to apply that holding to plaintiffs' Fourth Amendment claim was error because, for all the reasons previously stated, Congress has displaced the state secrets privilege with section 1806(f) in electronic surveillance lawsuits.

E. Even If Congress Had Not Displaced The State Secrets Privilege With Section 1806(f), The Privilege Would Not Provide An Alternative Ground For Summary Judgment

The district court's holding that the state secrets privilege was an alternative ground for dismissing plaintiffs' claim was error even if Congress had not displaced the state secrets privilege with section 1806(f).[52]

Dismissal was not warranted because even where the government successfully asserts the state secrets privilege, the result is "[t]he privileged information is excluded and the trial goes on without it." *General Dynamics*

[52] The Court reviews de novo the district court's application of the state secrets privilege. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc).

Corp. v. U.S., __ U.S. __, 131 S.Ct. 1900, 1906 (2011). "[T]he effect of the government's successful invocation of [the state secrets] privilege 'is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of evidence.'" *Al-Haramain*, 507 F.3d at 1204; *accord Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1082 (9th Cir. 2010) (en banc). "The plaintiff's case then *goes forward* based on evidence not covered by the privilege." *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) (emphasis added). As noted previously, in accordance with this rule the government agreed that the secret evidence it submitted could not be used to decide plaintiffs' standing or their Fourth Amendment claim. 12/19/14 Reporter's Transcript at 25-27, 42-45, 47; ECF No. 285 at 54-55; ECF No. 294-3 at 32-34; ECF No. 299-3 at 17 n.18, 20.

As with any privilege, the state secrets privilege excludes only evidence from a particular, privileged source, and does not prevent proof of relevant facts with evidence from a non-privileged source. *Mohamed*, 614 F.3d at 1090 (a "claim of privilege does not extend to public documents"). Moreover, "'[a]s in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence.'" *In re Sealed Case*, 494 F.3d 139, 147 (D.C. Cir. 2007).

Because plaintiffs' motion is based solely on public evidence, it is unaffected by any invocation of the state secrets privilege. Plaintiffs' evidence principally consists of public admissions by the government

regarding its Internet backbone surveillance; the declarations of Klein, Marcus, Russell, and plaintiffs; and AT&T's documents and its admission that it participates in FISA surveillance. The government long ago waived any privilege in any of the matters addressed in the Klein and Marcus declarations and the AT&T documents. *See Hepting v. AT&T Corp.*, 439 F.Supp.2d 974, 989 (N.D. Cal. 2006); ER 89-94 (6/23/06 Hearing Tr., *Hepting v. AT&T Corp.*, N.D. Cal. No. 06-cv-0672-VRW, ECF No. 284).

A ruling based solely on this public evidence discloses no state secrets, especially given the government's privilege waiver, the government's extensive admissions, and AT&T's disclosures. "Operational details," such as the identities of the government's surveillance targets, are irrelevant to the merits of plaintiffs' claims, and would not be revealed by a ruling in plaintiffs' favor. And to the extent that the government wished to use secret evidence to contest plaintiffs' evidence, it could have used section 1806(f)'s procedure.

F. The Valid-Defense Exception Does Not Apply Here

Below, the government sought to invoke the narrow "valid-defense" exception to the general rule that the lawsuit goes forward without the privileged evidence. Under the valid-defense exception, a lawsuit is dismissed instead of going forward if the secret evidence proves up "a valid defense." *Mohamed*, 614 F.3d at 1083 (internal quotation marks omitted).

Even if the state secrets privilege rather than section 1806(f) governed here, the valid-defense exception would not apply for two separate reasons:

First, the valid-defense exception does not apply because it is limited to government contracting cases.

Second, even if the state secrets privilege and the valid-defense exception both did apply here, they would require the government to submit evidence proving up a "demonstrably valid," and not just "plausible" or "colorable," defense. *In re Sealed Case*, 494 F.3d at 149-51, 153. The government did not prove up any "demonstrably valid" defense.

1. The Valid-Defense Exception Is Limited To Government Contract Claims

Under the valid-defense exception, secret evidence is not excluded but is used to the benefit of one party only—the defendant. This is contrary to the usual law of evidentiary privileges, under which all parties are deprived of the use of the privileged evidence and the chips fall where they may—a rule favoring neither plaintiff nor defendant.

The Supreme Court in *General Dynamics* made clear that the valid-defense exception is limited to government contract cases. The Court explained that the state secrets privilege it first recognized in *U.S. v. Reynolds*, 345 U.S. 1 (1953), is separate and distinct from the justiciability rules for government contract cases it has developed beginning with *Totten v. U.S.*, 92 U.S. 105 (1876), and extending through *Tenet v. Doe*, 544 U.S. 1 (2005), "two cases dealing with alleged contracts to spy." *General Dynamics*, 131 S.Ct. at 1906.

The *General Dynamics* Court explained first the limits of the state secrets privilege: "*Reynolds* was about the admission of evidence. It decided a purely evidentiary dispute by applying evidentiary rules: The privileged information is excluded and the trial goes on without it. . . . But the Court did not order judgment in favor of the Government." *General Dynamics*, 131 S.Ct. at 1906.

The Court next held that the source of the valid-defense exception is "the law of contracts"—"our common-law authority to fashion contractual remedies in Government-contracting disputes." *General Dynamics*, 131 S.Ct. at 1908, 1906; *see also id*. at 1907 ("Judicial refusal to enforce promises contrary to public policy"). It grounded the valid-defense exception in the ability of the parties to a government contract to allocate the risk that they will be unable to prove a contract breach claim because of the state secrets privilege.[53] *Id*. at 1909. Refusing to enforce government contracts in those circumstances "captures what the *ex ante* expectations of the parties were or reasonably ought to have been. . . . Both parties . . . must have assumed the risk that state secrets would prevent the adjudication of [their] claims . . . ." *Id.*

[53] Although this Court in *Mohamed* described (but did not apply) the valid-defense exception as a part of the *Reynolds* privilege (614 F.3d at 1083, 1087), this panel has authority to reconsider *Mohamed* because *General Dynamics* has "undercut the theory or reasoning underlying the prior circuit precedent in such a way that the cases are clearly irreconcilable." *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc).

Thus, dismissals under the valid-defense exception are limited to government contract cases. The reasoning underlying the exception has no application to claims not based on government contracts; plaintiffs never "assumed the risk" their Fourth Amendment rights would be unenforceable. In non-contract cases, "[t]he privileged information is excluded and the trial goes on without it." *Id*. at 1906.

2. Even If The Valid-Defense Exception Extended To Non-Contract Claims, The Government Did Not Establish A Valid Defense

Even if the state secrets privilege and not section 1806(f) governed here and even if the valid-defense exception applied to non-contract cases, it would not support summary judgment here because the government has not established a "demonstrably valid" defense. *In re Sealed Case*, 494 F.3d at 153.

Dismissal under the valid-defense exception requires that the state secrets privilege deprive the defendant of "information that would otherwise give the defendant a *valid* defense." *Mohamed*, 614 F.3d at 1083 (emphasis added, internal quotation marks omitted) (citing *In re Sealed Case*, 494 F.3d at 153). This is a high standard: "A 'valid defense' . . . is meritorious and not merely plausible and would *require* judgment for the defendant. 'Meritorious,' in turn, means 'meriting a legal victory.'" *In re Sealed Case*, 494 F.3d at 149 (citations omitted, emphasis added).

To determine whether the proposed defense is meritorious and requires judgment for the defendant, the district court must examine the privileged evidence and determine whether it proves the existence of the defense: "If the defendant proffers a valid defense *that the district court verifies upon its review of state secrets evidence*, then the case must be dismissed." *Id*. at 153 (emphasis added). This verification must be especially searching when, as here, the government is not an intervenor but a defendant simultaneously withholding evidence under the privilege while seeking dismissal on the ground that it has thereby crippled itself from presenting a valid defense.

The District of Columbia Circuit, in the decision *Mohamed* relied upon, explained why the defense must be proven by the secret evidence to be "demonstrably valid" and not just "plausible":

> Were the valid-defense exception expanded to mandate dismissal of a complaint for any plausible or colorable defense, then virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed. This would mean abandoning the practice of deciding cases on the basis of evidence—the unprivileged evidence and privileged-but-dispositive evidence—in favor of a system of conjecture.

In re Sealed Case, 494 F.3d at 149-50. Moreover, it "would run afoul of the Supreme Court's caution against precluding review of constitutional claims, see *Webster* [*v. Doe*], 486 U.S. [592,] 603-04 [(1988)], and against broadly interpreting evidentiary privileges." *Id*. at 151.

The government has not met its burden of establishing a demonstrably valid defense to plaintiffs' Fourth Amendment claim. The district court did not conclude the government had proven up a valid defense. Instead, it first found only that "any *possible* defenses" would require state secrets, a statement both insufficient and inaccurate, for the government defendants put forward numerous defenses in their public briefing not based on secret evidence. ER 6 (emphasis added). It next stated that that the government's "legal defenses are persuasive"—but to say that a secret defense never tested by the adversary process is "persuasive" is something significantly less than saying its validity has been proven. ER 13.

The district court ultimately concluded only that "a fair and full adjudication of the Government Defendants' defenses would require harmful disclosures of national security information"—again, not a finding that defendants have actually proven up a demonstrably valid defense. ER 13. The "full and fair adjudication" standard the district court put forward is not the law. Every evidentiary privilege—indeed, every rule that excludes relevant evidence—potentially makes the resulting adjudication something less than full and fair. Nonetheless, as with other privileges, when the state secrets privilege causes evidence to be excluded, the case proceeds using the remaining public evidence. *General Dynamics*, 131 S.Ct. at 1906.

Moreover, whether a defense is valid depends both on the facts and the legal standard governing the plaintiff's claim. Here, before the valid-defense exception could be applied, the Court would first need to

resolve the underlying legal dispute over what the Fourth Amendment requires in the circumstances alleged in plaintiffs' complaint—something that can be done entirely on the public record. Only once the Court had resolved that dispute would it then have the necessary legal standard against which to assess the validity of any proffered secret defenses.

Ultimately, there is no need to reach the valid-defense issue given that section 1806(f), and not the state secrets privilege, controls the use of secret evidence in this lawsuit and requires the case be decided on the merits.

CONCLUSION

The judgment should be reversed and the action remanded with directions to enter summary judgment in favor of plaintiffs on their Fourth Amendment Internet interception claim.

Dated: August 4, 2015

Respectfully submitted,

s/ *Richard R. Wiebe*
RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

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

THOMAS E. MOORE III
ROYSE LAW FIRM

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
JUSTINA K. SESSIONS
PHILIP J. TASSIN
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs-Appellants

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

This brief contains 13,943 words, excluding the parts of the brief exempted by Fed. R. App. Pro. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. Pro. 32(a)(5) and the type style requirements of Fed. R. App. Pro. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman.

s/ *Richard R. Wiebe*

Richard R. Wiebe
Counsel for Plaintiffs-Appellants

STATEMENT OF RELATED CASES

Fazaga v. Federal Bureau of Investigation, Nos. 13-55017, 12-56867, 12-56874 raises issues regarding the scope and application of 50 U.S.C. section 1806(f).

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on August 4, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: August 4, 2015

/s/ *Richard R. Wiebe*

STATUTORY AND CONSTITUTIONAL 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.

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 of 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 Act, 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.