CASE NO. 19-16066

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

PLAINTIFFS-APPELLANTS,

V.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

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

APPELLANTS' REPLY BRIEF

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

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

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

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

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

Counsel for Plaintiffs-Appellants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Constitutional Provisions

Legislative Materials

INTRODUCTION

In enacting laws in response to the Church Committee's revelations of unlawful government surveillance, Congress intended to enable Americans to challenge the legality of surveillance. Yet the government seeks to twist those laws into their exact opposite—laws erecting additional barriers to adjudication. But the secrecy-protecting procedures contained in section 1806(f) of FISA are a key instrument for enabling Americans to ensure that the government is conducting surveillance legally.[1] They must be applied to fulfill their purpose, as this Court held in *Fazaga v. FBI*, 916 F.3d 1202, 1230-38 (9th Cir. 2019).

The government also seeks to wield the state secrets privilege as a sword against establishing standing, even seeking to use it to block the courts from considering public evidence. But a court's ruling based solely on public evidence does not disclose state secrets, as this Court held in *Husayn v. Mitchell*, 938 F.3d 1123, 1132-34 & n.14 (9th Cir. 2019).

This Court must reject the government's clear attempt to pervert congressional intent, this Court's precedents, and the statutory language to block judicial consideration of its mass surveillance programs. *Fazaga* and *Husayn* firmly foreclose the government's central arguments.

[1] The provisions of 50 U.S.C. § 1806 are cited by section and subsection, e.g., "section 1806(f)." "FISA" is the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885c.

First, in *Fazaga*, the Court conclusively held that Congress in section 1806(f) completely displaced the state secrets privilege in electronic-surveillance cases and has forbidden any state-secrets dismissals. 916 F.3d at 1230-38. The Court reached this conclusion by carefully applying the traditional tools of statutory interpretation, examining section 1806(f)'s text and legislative history. *Fazaga* disposes of the government's untenable argument that plaintiffs' lawsuit can be dismissed under the state secrets privilege even if they demonstrate standing and aggrieved-person status using only public evidence.

Second, in *Husayn*, the Court held that, as common sense dictates, when a court decides an issue using only public evidence, it reveals no secrets and does not intrude on the state secrets privilege. 938 F.3d at 1132-34 & n.14. Thus, even if section 1806(f) did not displace the state secrets privilege, *Husayn* disposes of the government's equally untenable argument that the privilege bars courts from making rulings based on public evidence.

Because plaintiffs have demonstrated their standing and aggrieved-person status using only public evidence, the judgment must be reversed. Even without resort to the secret evidence or section 1806(f)'s procedures, plaintiffs have presented abundant public evidence from which a factfinder could easily conclude it is more probable than not that the government caused their Internet communications to be copied and diverted and that it is more probable than not that the government collected their phone records and Internet metadata. That is all that Article III standing requires, and it

also demonstrates that plaintiffs are aggrieved persons entitled to use section 1806(f).

The public evidence includes government disclosures, eyewitness testimony, expert testimony, and documents, including documents of plaintiffs' telecommunications provider AT&T. It confirms what has been apparent to all the world for a very long time: the government's surveillance programs and their impact on ordinary Americans is no secret. Neither is AT&T's participation.

Moreover, the secret evidence supporting plaintiffs' standing and aggrieved-person status is an additional ground on which the judgment must be reversed. Sections 1806(f) and 2712(b)(4) direct the Court to consider the secret evidence as well as the public evidence.[2] *Fazaga* makes clear that section 1806(f)'s preemption of the state secrets privilege is absolute, and leaves no room for the state secrets privilege. And, having displaced the state secrets privilege, section 1806(f) does not erect additional threshold barriers in the form of proving standing or aggrieved-person status before its procedures can be used. *Fazaga* directed that on remand the plaintiffs in that lawsuit were entitled to use section 1806(f)'s procedures, even though at that point all they had established were well-pleaded allegations of electronic surveillance.

[2] 18 U.S.C. § 2712 is cited as "section 2712" or with a subsection, e.g., "section 2712(b)(4)."

Finally, plaintiffs have proven the government violated their Fourth Amendment rights by its Upstream interception and searching of their Internet communications. Four years ago, in rejecting as premature plaintiffs' appeal of their Fourth Amendment claim, the Court determined that claim should be decided in this appeal from the final judgment. Although the government refuses to defend the constitutionality of its Upstream Internet interception program, that does not defeat this Court's power and obligation to decide the issue now.

ARGUMENT

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

The government's most extreme argument is that even when a plaintiff challenging unlawful electronic surveillance successfully establishes standing and aggrieved-person status using public evidence, the government may nonetheless compel dismissal by asserting that litigating those issues using public evidence will reveal state secrets.[3] GB 17, 18-19, 27-29, 34-35. This is the ground on which the district court dismissed plaintiffs' lawsuit. Appellants' Excerpts of Record (ER) 27.

The government presents no authority in support of this argument, by which the government would replace the courts as the gatekeeper of sections 1806(f) and 2712(b)(4) in lawsuits challenging government surveillance.

[3] "The government" includes all defendants, including the personal-capacity defendants. Government Brief ("GB") 8 n.1.

This argument is foreclosed by *Fazaga* and by the text and legislative histories of sections 1806(f) and 2712(b)(4). Appellants' Opening Brief (AOB) 15-21.

A. As *Fazaga* Holds, Congress Has Forbidden State-Secrets Dismissals In Electronic-Surveillance Cases

Mohamed v. Jeppesen provides that in rare circumstances a lawsuit can be dismissed under the state secrets privilege if "'litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets.'" *Fazaga*, 916 F.3d at 1227-28 (quoting *Mohamed v. Jeppesen*, 614 F.3d 1070, 1083 (9th Cir. 2010) (en banc)).

That principle has no application to plaintiffs' claims. As this Court held in *Fazaga* and as the AOB explains, in sections 1806(f) and 2712(b)(4) Congress completely displaced the state secrets privilege in lawsuits challenging electronic surveillance. Congress instead created a secure procedure for courts to receive national-security evidence and use it to decide the plaintiff's claims. AOB at 15-18.

"FISA displaces the dismissal remedy of the common law state secrets privilege as applied to electronic surveillance generally," no matter what the constitutional or statutory source of the plaintiff's claim. *Fazaga*, 916 F.3d at 1226, 1238; *see also id*. at 1230-34.

Section 2712(b)(4) extends the complete displacement of the state secrets privileges to plaintiffs' communications records claims under the

Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. AOB 17-18.

Fazaga repeatedly and unequivocally holds that section 1806(f)'s displacement of the state secrets privilege is "mandatory" and "exclusive" for all claims challenging electronic surveillance. *Fazaga*, 916 F.3d at 1237, 1231. Thus, the government's argument that state secrets dismissals are permissible in electronic-surveillance cases even where the plaintiff can prove standing and aggrieved-person status with public evidence must be rejected.

The government ignores not only *Fazaga* but FISA's legislative history in asserting that the state secrets privilege applies to plaintiffs' claims: "[T]he plain language, statutory structure, and legislative history" of section 1806(f) "demonstrate that Congress intended FISA to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance." *Fazaga*, 916 F.3d at 1238.

FISA has its origins in the Church Committee's investigation into the government's unlawful surveillance of innocent Americans during the Cold War. *Fazaga*, 916 F.3d at 1233. The Church Committee called for civil remedies that would permit ordinary Americans to challenge any future unlawful surveillance even in the face of government claims of secrecy. *Id*. FISA, and section 1806(f) in particular, was Congress's implementation of the Church Committee's recommendations. *Id*. at 1233-34.

Fazaga observes that section 1806(f)'s procedures protect state secrets from public disclosure by requiring *ex parte* and *in camera* review of secret evidence. *Fazaga*, 916 F.3d at 1234. The government strains to contort this commonplace observation into an endorsement by *Fazaga* of state-secrets dismissals, GB 28-29, but that attempt fails in light of *Fazaga's* repeated and unequivocal statements holding that section 1806(f)'s procedures completely displace the state secrets privilege and forbid any state-secrets dismissals. AOB 15-18. Section 1806(f) protects government secrets not, as the government would have it, by excluding them under the state secrets privilege and then railroading the case to dismissal, but by protecting them with *ex parte* and *in camera* procedures while the Court uses them in deciding the plaintiff's claims on their merits.

B. Congress Did Not Give The Government Control Over Litigation Challenging Unlawful Electronic Surveillance

Permitting state-secrets dismissals of electronic-surveillance lawsuits would give the government control over whether it could be sued for unlawful surveillance whenever the case involved national-security evidence. But that is contrary to the statutory scheme established by Congress.

Not only section 1806(f) and *Fazaga* but also section 2712 show that Congress did not give the government control over whether a plaintiff could seek relief for unlawful surveillance. In section 2712, Congress expressly considered what preconditions to suit to impose. It did require that a

plaintiff first present their claim administratively to the government as a precondition to filing suit. § 2712(b)(1), (b)(2). Congress easily could have also required the government grant its consent as a precondition to bringing suit. Congress did not.

Likewise, Congress easily could have required that lawsuits under section 2712 be subject to the state secrets privilege. It chose the opposite course, however, displacing the state secrets privilege by mandating that the procedures of section 1806(f) govern state secrets in Wiretap Act (18 U.S.C. §§ 2510-2522) and SCA cases "[n]othwithstanding any other provision of law," including the common-law state secrets privilege. § 2712(b)(4).

II. *Fazaga* Makes Clear That Proof Of Standing And Aggrieved-Person Status Is Not A Precondition To Using Section 1806(f)

As a fallback, the government argues that plaintiffs must prove standing and aggrieved-person status using public evidence before the district court may use the procedures of section 1806(f). GB 16. That argument fails both factually and legally:

First, as a factual matter, plaintiffs have presented ample public evidence proving their standing and aggrieved-person status, so if that proof is required as the government contends, plaintiffs have met their burden. This evidence is discussed at pages 25-58 and 79-88 of the AOB; it is further discussed in section III below. A factfinder could easily conclude from the public evidence that it is more probable than not that the government caused their Internet communications to be copied and diverted from their normal

course of transmission and that it is more probable than not that the government collected their phone records and Internet metadata. Because plaintiffs have demonstrated their standing and aggrieved-person status using public evidence, the judgment must be reversed for that reason alone.

Second, as a legal matter, sections 1806(f) and 2712(b)(4) do not impose on plaintiffs the threshold burden of proving standing and aggrieved-person status. They embrace within their scope these plaintiffs, who do not just allege unlawful electronic surveillance in a well-pleaded complaint that has survived a motion to dismiss, but who have submitted substantial supporting evidence demonstrating that their Internet communications have been intercepted and their communications records have been collected. A plaintiff who has done so, as plaintiffs here have, is entitled to proceed to the merits using the procedures of sections 1806(f) and 2712(b)(4).

The Church Committee's fundamental goal in its recommendations was preventing unlawful surveillance of ordinary, innocent Americans, and providing them with an effective avenue of judicial relief if it ever occurred. *Fazaga*, 916 F.3d at 1233-34. The drafters of FISA heeded the Committee's recommendations. *Id*. Plaintiffs present the paradigmatic case at the heart of FISA and the Church Committee's concerns: innocent Americans subjected to suspicionless mass surveillance. Congress intended sections 1806(f) and 2712(b)(4) to offer persons in plaintiffs' position the procedural tools to obtain effective redress while protecting national security. *Fazaga*, 916 F.3d at 1233-34. To say that they are barred from using section

1806(f)'s procedures to obtain relief would be a complete nullification of Congress' intent and an abdication of the judicial responsibility to faithfully apply the statutory commands of sections 1806(f) and 2712(b)(4).

A. Section 1806(f) Does Not Require Proof Of Standing Or Aggrieved-Person Status

As the AOB explains at pages 22-24, *Fazaga* held that a plaintiff who has made well-pleaded allegations of unlawful electronic surveillance is an aggrieved person entitled to use section 1806(f). *Fazaga*, 916 F.3d at 1216, 1238-39, 1251. The Court found that the "[p]laintiffs are properly considered 'aggrieved' for purposes of FISA" (*id*. at 1238-39) because they alleged in detail that they were subjected to surveillance (*id*. at 1216).

Accordingly, the *Fazaga* Court remanded the case for a determination of the merits, including the lawfulness of the surveillance, "using § 1806(f)'s *ex parte* and *in camera* procedures" to review national-security evidence. *Fazaga*, 916 F.3d at 1251. The Court did not require as a precondition to reaching the merits that the plaintiffs first prove that they were aggrieved using only public evidence. And properly so, because whether plaintiffs are aggrieved persons "is a merits determination, not a threshold standing question." *Jewel v. NSA*, 673 F.3d 902, 907 n.4 (9th Cir. 2011).

This is as the Church Committee intended. As *Fazaga* explains, the Church Committee intended that the *in camera* procedures that became section 1806(f) would "'allow plaintiffs with substantial claims to uncover enough factual material to argue their case.'" 916 F.3d at 1233 (quoting

Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, 337 (1976)). The Committee explained that a "substantial claim" was one in which the plaintiff had "allege[d] specific facts which indicate that he was the target of illegal intelligence activity." S. Rep. No. 94-755, 338 n.70.

Fazaga notes that the *Fazaga* plaintiffs' electronic surveillance claims might "drop out of consideration" if they fail to prove them up in future proceedings on the merits. 916 F.3d at 1253. The government misreads this as a statement that the plaintiffs must first prove their aggrieved-person status with public evidence before section 1806(f)'s procedures may be used. GB 27-28. But that contention fails because it has no basis in the Court's statement and because *Fazaga* explicitly directs that those future proceedings on the merits shall use section 1806(f)'s procedures, without requiring any further proof of aggrieved-person status. 916 F.3d at 1251; *see also id*. at 1238-39; AOB 22-23.

Fazaga's holding is well grounded in section 1806(f). Under FISA, an "aggrieved person" is simply "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Congress' intent in creating the "aggrieved person" standard was not to limit the operation of section 1806(f) but to make FISA's substantive remedies "coextensive, but no broader than, those persons who have standing to raise claims under the

Fourth Amendment with respect to electronic surveillance." H.R. Rep. No. 95-1283, pt. 1, at 66 (1978) (ECF No. 90, Ex. H). The purpose of the "aggrieved person" definition was simply to exclude from FISA's remedies those who were not parties to the intercepted communication, because Congress had "no intent to create a statutory right in such persons." *Id*.

In section 1806(f), "aggrieved person" is merely a description of a person with an unlawful surveillance claim who makes a discovery request. 1806(f) ("whenever any . . . request is made by an aggrieved person . . . to discover . . . materials relating to electronic surveillance"); *see also* H.R. Rep. No. 95-1283, pt. 1, at 93 (1978) (use of section 1806(f) "may, for example, arise incident to a discovery motion in a civil trial"). A plaintiff may propound discovery without first proving up standing or the merits.

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

Because it is the government, not the plaintiff, that triggers section 1806(f), the plaintiff does not have to prove anything to trigger its operation.

Unless the government asserts that secret evidence is at issue, discovery continues along its ordinary course, evidence is disclosed, and section 1806(f) never comes into play. If the government makes the assertion, then the court must preserve the necessary secrecy by implementing section 1806(f)'s *ex parte*, *in camera* review procedures but must use the secret evidence to decide the case.

U.S v. Cavanagh, 807 F.2d 787 (9th Cir. 1987), does not support the government's position. *Cavanagh* did not hold that a plaintiff must establish aggrieved-person status "as a threshold matter" before a court can use section 1806(f), as the government contends. GB 28. Instead, it held that "as a threshold matter" in Cavanagh's appeal *the parties did not dispute that Cavanagh had standing* under section 1806(e) to challenge the government's introduction of surveillance evidence in his criminal case and was an aggrieved person: "As a threshold matter, there is no dispute over appellant's standing to challenge the lawfulness of the surveillance. FISA permits aggrieved persons to seek suppression of evidence on the ground that it was unlawfully acquired or that the surveillance was not conducted in conformity with the order of authorization. *Id*. § 1806(e). Appellant was a party to an intercepted communication, and the government concedes he is an 'aggrieved person' within the meaning of the statute." *Cavanagh*, 807 F.2d at 789. Further, in *Cavanagh* the government submitted secret

evidence to the Court pursuant to section 1806(f), as section 1806(f) required it to do.[4] *Id.*

B. Section 2712(b)(4) Has No Standing Or Aggrieved-Person Precondition

Moreover, section 2712(b)(4) has no aggrieved-person precondition. It applies in this lawsuit together with section 1806(f). Section 2712(b)(4) permits the use of secret evidence for any purpose, including proving standing.

Plaintiffs are aggrieved persons under section 2712 because their allegations are more than sufficient to commence an action. Under section 2712, an aggrieved person is simply someone with well-pleaded allegations of a Wiretap Act or SCA violation, not someone who has proven up their standing or the fact that they were surveilled. Section 2712 provides that an "any person who is aggrieved" by a Wiretap Act or SCA violation "may commence an action." § 2712(a). But proof is not necessary to commence an action, only well-pleaded allegations.

Section 2712(a) goes on to describe the remedies available "if a person who is aggrieved successfully establishes such a violation." *Id.* In doing so, section 2712(a) clearly distinguishes someone "who is aggrieved"

[4] The government cites *Wikimedia Foundation v. NSA* (GB 25), but to no avail because the *Wikimedia* district court made the same analytic errors as the district court below. 335 F. Supp. 3d 772, 786 (D. Md. 2018); *later op.*, No. 1:15-CV-662, 2019 WL 6841325, at *22-*23 (D. Md. Dec. 16, 2019).

because he or she has allegations sufficient to "commence an action" from someone who has gone on to "successfully establish[]" a violation. *Id*.

Once the action is commenced, any secret evidence[5] must be reviewed using "the procedures set forth in section 1[8]06(f)" and not excluded, "[n]otwithstanding any other provision of law," including the state secrets privilege. § 2712(b)(4). Section 2712(b)(4)'s requirement to use section 1806(f)'s procedures is "exclusive," regardless of the purpose for which the evidence is used, whether standing or the merits. *Id*.

Section 2712(b)(4) by its express terms incorporates only section 1806(f)'s evidence-review procedures—"the procedures . . . by which [secret evidence] . . . may be reviewed," i.e., *ex parte* and *in camera* review by the district court. § 2712(b)(4). Its text does not incorporate any preconditions to using those procedures from section 1806(f). Thus, there is no support for the government's argument that section 2712(b)(4) incorporates not only section 1806(f)'s evidence-review procedures but also the government's purported requirement that a plaintiff prove they are an aggrieved person. GB 33-34.

C. *Clapper's* Dicta Has No Application Here

There is no merit to the government's attempt to use dicta from a footnote in *Clapper v. Amnesty International*, 568 U.S. 398, 412 n.4 (2013),

[5] Section 2712(b)(4) applies to secret evidence because it applies to "materials governed by" section 1806(f) (i.e., secret evidence whose "disclosure . . . would harm the national security," § 1806(f)).

to defeat Congress's command in sections 1806(f) and 2712(b)(4). The dicta has no application to the quite different facts of this case.

This Court has already distinguished *Clapper's* facts from this case. *Jewel*, 673 F.3d at 911. *Clapper* was not a section 1806(f) case or a state-secrets case. It was a standing case in which the plaintiffs alleged potential future harm, not actual existing harm as the *Jewel* plaintiffs allege. Additionally, it was a pre-enforcement challenge to potential future *targeted* surveillance, not a challenge to actual *untargeted* mass surveillance as is this lawsuit.

The *Clapper* plaintiffs' theory of standing relied on a long chain of possibilities about what might happen in the future: They alleged that foreign persons with whom they communicated were likely to be targeted for surveillance, and that the plaintiffs' communications were likely to be collected incidentally to that conjectured targeted surveillance of others.

When a plaintiff alleges standing not based on past and ongoing harm, as the *Jewel* plaintiffs do, but on potential harm in the future, they must meet the high standard of showing that the potential future harm is not just possible but is "certainly impending." *Clapper*, 568 U.S. at 409. *Clapper* held that the plaintiffs there lacked sufficient evidence to prove that the potential capture of the plaintiffs' future communications by the conjectured future surveillance of those with whom they might communicate in the future was "certainly impending." 568 U.S. at 410-14.

The government relies on dicta in footnote 4 of *Clapper*, in which the Court discussed a "hypothetical disclosure proceeding" (not sections 1806(f) or 2712(b)(4)) in which the government would disclose *in camera* whether a plaintiff's communications had been targeted and intercepted. 568 U.S. at 412 n.4. The Court hypothesized that if a terrorist were to file suit alleging they had been targeted and used this hypothetical procedure, "the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets." *Id*.

There is no such risk here, and *Clapper's* dicta has no application to this lawsuit. Unlike *Clapper*, plaintiffs are challenging *un*targeted mass surveillance. The identities of the government's surveillance targets, the search terms used by the government, and other operational details are irrelevant to plaintiffs' claims, and would not be revealed by a ruling in plaintiffs' favor, even if that ruling were based on both public and secret evidence.

Plaintiffs' theory of standing is *not* that they were targets or that those they communicate with were targets. It is that they are innocent, untargeted Americans caught up in the government's mass surveillance programs. So a holding that "plaintiffs have standing" or that "plaintiffs lack standing" says nothing about whether plaintiffs or anyone else is on the list of surveillance targets. Likewise, a ruling on the merits would not disclose who the government's targets are.

Moreover, *Clapper* did not address sections 1806(f) or 2712(b)(4). *Clapper* made no suggestion that courts have any authority to refuse to apply validly-enacted statutes governing the courts like sections 1806(f) and 2712(b)(4). Congress's judgment was that the protection of individual liberty required that unlawful-surveillance claims be litigated on the merits, not dismissed, and section 1806(f)'s procedures were the means by which it balanced the protection of individual liberty with the protection of national security. *Fazaga*, 916 F.3d at 1233.

The alternative—permitting the Executive to conduct unlawful and unconstitutional mass surveillance of hundreds of millions of Americans without any judicial recourse—was decisively rejected by Congress. State-secrets "dismissal[s] . . . would undermine the overarching goal of FISA more broadly—'curb[ing] the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it.'" *Fazaga*, 916 F.3d at 1237 (quoting S. Rep. No. 95-604, pt. 1, 8 (1978)). Refusing to apply sections 1806(f) and 2712(b)(4) would abdicate the Judiciary's Article III responsibility to adjudicate the constitutional and statutory limits on surveillance.

D. Ruling On Plaintiffs' Standing And Aggrieved-Person Status Would Not Require Disclosing The Underlying Secret Evidence

1. Section 1806(f) Proceedings Do Not Disclose Secret Evidence

Because this Court determines de novo the issues on appeal, including all issues relating to the state secrets privilege, the district court's conclusion that "permitting further proceedings would jeopardize national security" (ER 27) is of no moment, and the government's heavy reliance on it does nothing to advance its position. *Jeppesen*, 614 F.3d at 1086; *Al-Haramain Islamic Foundation v. Bush*, 507 F.3d 1190, 1202-04 (9th Cir. 2007). Given this Court's de novo review, there is no need for plaintiffs to challenge that conclusion, but it lacks merit in any event.

The district court made a fundamental error in repeatedly stating that determining plaintiffs' standing, aggrieved-person status, or their claims using section 1806(f)'s procedures would require "disclosure" of the secret evidence. ECF 462 at 18-20, 24-25. "Critically, the FISA approach does not publicly expose the state secrets." *Fazaga*, 916 F.3d at 1234. Section 1806(f), by providing for *in camera*, *ex parte* review of the secret evidence, keeps the secret evidence secret and does not require public disclosure.

A district court can entirely avoid any disclosure of secret evidence by considering it *ex parte* and *in camera* and not discussing it in its public decision. The district court can and should make disclosures of secret evidence to plaintiffs under secure conditions to permit them to litigate their

case. § 1806(f). But that, too, does not publicly disclose the secret evidence.

Just as important, the details of the government's surveillance programs—e.g., the identities of its targets, the selector terms used in searching for communications and records of interest—are irrelevant to plaintiffs' claims and would not be disclosed by a ruling on the merits of plaintiffs' claims. The district court need not even review those details in order to rule on plaintiffs' claims.

Not only can the district court avoid entirely any disclosure of secret *evidence,* it can structure its proceedings and its rulings to avoid disclosure of *facts* the government contends are secret. For example, it can receive evidence going to both standing and the merits in a single proceeding. *Rosales v. U.S.*, 824 F.2d 799, 803 (9th Cir. 1987). If the plaintiff lacks standing, a one-line public ruling stating "Plaintiff's claims are dismissed." does not reveal whether the plaintiff was subject to surveillance but the surveillance was legal or instead was not subject to surveillance at all. The district court can discuss the secret evidence and its reasoning in a secret opinion.

If it finds both that the plaintiff has standing and that the surveillance was unlawful, a one-line public ruling "Judgment for plaintiff." is a judicial finding that the plaintiff was surveilled unlawfully. But that is as Congress intended. By creating claims for unlawful national-security surveillance and the means to litigate those claims, Congress intended that unlawful

surveillance conducted by the government would be publicly exposed. And, again, the district court can discuss the secret evidence supporting its conclusion in a secret opinion.

Moreover, as discussed in section III below, many of the facts the government contends are secret have long been publicly disclosed, some officially and some unofficially. And, as explained next, a judicial finding based on public evidence does not disclose any state secrets, nor is it the same as an executive-branch confirmation of a secret fact. *Husayn*, 938 F.3d 1123 at 1132-34 & n.14.

2. Proceedings Using Only Public Evidence Do Not Disclose State Secrets

Any ruling based solely on the public evidence discloses no state secrets, even if it finds plaintiffs have established their standing. The judicial function of drawing inferences and conclusions from public evidence does not transmute the result into a state secret. This is true even if the public evidence leads to the same conclusions as an analysis of the secret evidence would.

This Court recently explained that a court's factual determinations in judicial proceedings are not the equivalent of an Executive Branch confirmation that a fact is true. *Husayn* addressed discovery into a CIA torture site in Poland, whose location the government claimed was a state secret but which has been the subject of media reports and other disclosures. This Court rejected the government's assertion that permitting discovery of

government contractors regarding the CIA site would be the equivalent of "official confirmation" of the site's existence: "The conclusion that the existence of a CIA site in Poland is not a secret is not equivalent to a finding, either by the district court or this court, that the government has taken any official position on the existence of such a facility." *Husayn*, 938 F.3d at 1133.

Moreover, given the extensive public disclosures of the facts underlying *Husayn*, "insofar as the government asserts privilege over the basic fact that the CIA detained Abu Zubaydah in Poland and that he was subjected to torture there, this certainly does not protect the disclosure of secret information, but rather prevents the discussion of already disclosed information in a particular case." *Id*. "These facts have been in the public eye for some years now" through unofficial disclosures, "and we find no reason to believe that [government contractors] testifying about these facts 'will expose ... matters which, in the interest of national security, should not be divulged.'" *Id*. at 1134 (quoting *U.S. v. Reynolds*, 345 U.S.1, 10 (1953)).

"We cannot agree . . . that Article III judges are 'not in a position' to reach conclusions with publicly available facts." *Id*. at 1132 n.14.

As in *Husayn*, a decision on plaintiffs' standing or on the merits based on the public evidence would do nothing to disturb any ambiguity the government contends exists from the lack of an official confirmation that it conducts the surveillance that plaintiffs allege. It would only represent the district court's assessment of the public evidence before it, which is all that

any court judgment ever represents, and not a confirmation by the government.

In particular, as in *Husayn*, the facts that the government contends are secret have long been in the public domain, as the public evidence laid out in the AOB demonstrates. These include: AT&T's and Verizon's participation in the government's surveillance program; the government's acquisition of phone records from AT&T and Verizon; the wholesale copying and searching of communications flowing through AT&T's backbone junctions; and the collection of Internet metadata from AT&T.

The government's contention that judicial findings based on these public facts would threaten national security is wrong. Just as Poland's participation in the CIA's torture program is not a secret despite the government's refusal to acknowledge it, so, too, here, AT&T's and Verizon's participation in the government's surveillance programs is not a secret despite the government's refusal to acknowledge it. (Indeed, both AT&T and Verizon admit that they conduct national security surveillance under FISA on behalf of the government. ER 911, 913, 927, 929.) Judicial findings based on plaintiffs' public evidence disclose nothing new and do not harm national security. *Husayn*, 938 F.3d at 1132-34. Nor are they the equivalent of a government confirmation that the findings are true. *Id*. at 1133.

III. Plaintiffs Have Demonstrated Using Public Evidence That They Have Standing And Are Aggrieved Persons

Even if the government were correct that before a court may use section 1806(f)'s procedures a plaintiff must first establish their standing and aggrieved-person status using public evidence, plaintiffs here have done so. For that reason, the Court ultimately need not decide whether a plaintiff proceeds forward under section 1806(f) or section 2712(b)(4) by presenting well-pleaded allegations, or by proving with public evidence it is more probable than not that they have standing and are aggrieved, because the record includes both.

The standards for evaluating evidence in the context of summary judgment apply here just as they do in every other case: The evidence must be viewed in the light most favorable to plaintiffs. It must be evaluated as a whole, each item supporting and reinforcing the others. And it only need show it is more probable than not that plaintiffs have standing and are aggrieved, and not meet any higher standard of proof. AOB 24-26.

The government's attacks on plaintiffs' evidence lack merit. The government also fails to view the evidence in the light most favorable to plaintiffs and fails to address its cumulative impact. Instead, it dissects the evidence and views it narrowly in the light most favorable to itself.

A. The Public Evidence Shows Plaintiffs' Standing For Their Phone Records Claims

As the AOB explains, plaintiffs' public evidence establishes that their phone records were acquired by the government. AOB 26-36. The

government focuses its attack on the NSA Letter and the NSA Draft OIG Report. These documents are admissible and are supported by other evidence as well.

1. The NSA Letter

The NSA Letter is a public document disclosed by the government to the *New York Times* and published by the *Times* in its entirety.[6] AOB 27-28, 33-35. The NSA Letter alone is sufficient to establish plaintiffs' standing and aggrieved-person status for their phone records claims. It is admissible, and the district court abused its discretion in excluding it. AOB 33-35.

The government does not deny that it disclosed the NSA Letter to the *Times* but contends that it should nonetheless be treated as secret and barred by the state secrets privilege. GB 43-45.

Even apart from sections 1806(f) and 2712(b)(4)'s displacement of the privilege, the government's assertion of the state secrets privilege fails because the NSA Letter is public, and a "claim of privilege does not extend to public documents." *Jeppesen*, 614 F.3d at 1090. "[I]n order to be a 'state secret,' a fact must first be a 'secret.'" *Husayn*, 938 F.3d at 1133. There is nothing secret about the contents of the NSA Letter.

[6] The government is mistaken in suggesting (GB 44, 45) the *Times* published only an article about the NSA Letter, and not the letter itself. The article links to the letter and it remains available on the *Times'* website. *See* p. 111 at https://www.nytimes.com/interactive/2015/08/12/us/nsa-foia-documents.html.

And there is no doubt the NSA Letter is an authentic government document. The NSA Letter is authenticated by the government's production of it in litigation to the *Times* and independently by the declaration of *Times* counsel David McCraw, a witness with personal knowledge who testifies to receiving the NSA Letter directly from the government. AOB 34-35; ER 147-48.

Jeppesen and *Husayn* thus foreclose the government's attempt to force the Court to pretend that the contents of the NSA Letter are secret. *Al-Haramain Islamic Foundation v. Bush* does not support the government because the government recovered the *Al-Haramain* "Sealed Document" before any public disclosure, and its contents "'remain[] secret.'" 507 F.3d at 1202. Here, the facts are the opposite: the government sought no judicial relief to prevent the *Times* from publishing the NSA Letter, and the *Times* published it. AOB 34.

2. The NSA Draft OIG Report

As the AOB explains, the evidence amply authenticates the NSA Draft OIG Report, and the district court abused its discretion in excluding it. AOB 29, 35-36.

The government erroneously argues that the district court excluded Snowden's testimony authenticating the NSA Draft OIG Report. GB 43. The district court did not exclude Snowden's testimony but found its weight insufficient to authenticate the NSA Draft OIG Report: "Plaintiffs' contention that Snowden may authenticate the purported NSA document is

not persuasive, either by way of his current declaration or in the future through live testimony."[7] ER 19. Whether evidence is "persuasive" speaks to its weight, not its admissibility.

Snowden's declaration is more than sufficient to meet the low bar of authentication. It satisfies Federal Rule of Evidence 901(b)(7)(B) by demonstrating that the NSA Draft OIG Report "is from the office where items of this kind are kept."

The government contends that Rule 901(b)(7)(B) is limited to publicly available documents. GB 48. But the rule contains no such limitation and is much broader than that. It covers any "public record or statement" (in contrast to a private document that may happen to be in a government file) maintained by any "public agency," whether or not the public has access to the document. *Id*. Moreover, "'record' includes a memorandum, report, or data compilation." Fed. R. Evid. 101(b)(4). Thus, Rule 901(b)(7)(B) easily covers the NSA Draft OIG Report.

Moreover, Rule 901 does not require authentication by a custodian, "only personal knowledge that a document was part of an official file," which Snowden has. *U.S. v. Estrada-Eliverio*, 583 F.3d 669, 673 (9th Cir. 2009). Thus, the government errs in asserting that Snowden cannot

[7] Snowden's absence from the United States is no barrier to his testimony at trial, either by video or other remote means or by letter rogatory. Fed. R. Civ. P. 28(b), 30(b)(4), 43(a). *See* ECF No. 441-3 at 2-3.

authenticate the NSA Draft OIG Report because he was not its custodian. GB 48-49.

3. Additional Evidence Also Supports Plaintiffs' Standing

As the AOB details, plaintiffs have provided additional evidence supporting their standing. AOB 27-32.

The government critiques the Privacy and Civil Liberties Oversight Board's (PCLOB's) calculations of the scope of the phone records program, dismissing them as airy, unfounded speculation. GB 39-40. But the PCLOB is a serious government organization charged with honestly and accurately explaining the phone records program to the American people, and its calculations are very conservative and well-supported.

The phone records program maintained five years of records from each phone company on each of its customers; the PCLOB assumed that the average customer called only 75 different people during those five years, obviously a gross underestimate. ER 180, 184. Based on this assumption, and on the government's admission that it made around 300 three-hop queries of the phone records database in 2012, the PCLOB calculated (as a matter of simple mathematics without the need for further assumptions) that those queries yielded the phone records of 120 million persons. ER 185-86.

Importantly, the 120 million phone numbers was the *output* of the government's queries; the *input*—the raw phone records data of all the participating phone companies' customers—was necessarily even larger.[8]

The government next cites *Clapper* in a misguided attempt to show that any conclusions drawn from the government's disclosures regarding the size and methods of the phone records program are conjectural. GB 41-42. But *Clapper* applied the rigorous standard of proof for *future* injury, which requires proof that future injury is not just probable but "certainly" impending. *Clapper*, 568 U.S. at 409. The evidence in *Clapper*—much weaker than the evidence presented here because it required speculation about the future intentions and actions of the government, the FISA Court, and third parties—did not meet that high standard. *Id.* at 410-14.

Plaintiffs' claims, however, are of *past* injury and their evidence need only meet the lower, more-probable-than-not, preponderance standard of civil litigation. And the conclusions drawn from the government's

[8] The government compares the number of AT&T's and Verizon's subscribers to the total count of U.S. phone numbers in an attempt to show that a very large phone records program could operate without AT&T and Verizon. GB 40 n.8. But that attempt fails because it is an apples-to-oranges comparison: many subscribers have multiple phone lines. Businesses do, and so do many families with three, four, five (or more) cell phones under a single account. So the active phone numbers of AT&T's and Verizon's subscribers are far more numerous than the subscribers themselves.

disclosures must be considered in conjunction with the direct evidence of the NSA Letter and the NSA Draft OIG Report.

The government is also incorrect in asserting that plaintiffs make a probabilistic standing argument: plaintiffs do not argue that the government acquired only some of AT&T's records and that theirs were probably among those acquired, but have shown instead that the government acquired all of AT&T's records, including theirs. GB 41. It is undisputed that for those telephone companies subject to the call records program, call records were acquired for all of their customers. Thus, once it is shown that it is more probable than not that a particular company was subject to the call records program, it is certain, and not merely "probabilistic," that each customer's call records were collected.[9]

Finally, the government's reliance on *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015), lacks merit for all of the reasons explained at AOB 32-33, none of which the government addresses. GB 42-43.

[9] Equally erroneous is the government's argument that plaintiffs must prove "either that the government collected *all* metadata of all telephone calls in the United States" or "actually sought and collected metadata about plaintiffs' particular calls." GB 37. The hole in the government's logic is that plaintiffs may establish standing, as they have, by showing that the government collected metadata for all calls of their particular phone companies, AT&T and Verizon.

B. The Public Evidence Shows Plaintiffs' Standing For Their Upstream Internet Interception Claims

To establish their standing, plaintiffs need only show the initial copying and diversion of their Internet communications, fairly traceable to the government. AOB 42-43. That alone is an "identifiable trifle" sufficient for standing. *U.S. v. SCRAP*, 412 U.S. 669, 689 n.14 (1973). The government is wrong to contend that plaintiffs need also prove what happens in the secret SG3 room, or how and where their communications are filtered and scanned. GB 57. What happens to plaintiffs' communications after the initial copying and diversion is irrelevant to standing.

The government also errs in arguing that plaintiffs must show "the NSA had control and direction over AT&T property and personnel in the SG3 room." GB 59. As it conceded below, for the copying and diversion of their communications to be fairly traceable to the government, plaintiffs need only show "that AT&T conducted the activities to which they attribute their injuries as part of the NSA's surveillance process." ECF No. 439 at 8.

Although framed as an attack on the admissibility of plaintiffs' evidence, many of the government's objections really go to the weight of plaintiffs' evidence.

The government's arguments attacking the weight of plaintiffs' evidence supporting their Internet interception claims ignore that this is summary judgment, where the evidence must be viewed in the light most favorable to plaintiffs and where all inferences must be drawn in plaintiffs'

favor. And it must be viewed as a whole, not as fragments weighed in isolation. A reasonable factfinder, looking at the public evidence as a whole, each item supporting and corroborating the others, could easily conclude that plaintiffs' communications more likely than not have been intercepted, giving plaintiffs standing.

1. Evidence From AT&T And Its Employees

a. The Klein Declaration

The government attacks the percipient evidence of Mark Klein. But it fails to respond to the host of authority cited by plaintiffs explaining why Klein's testimony about the activities of his employer AT&T and his co-workers is admissible. AOB 49-53. And contrary to the government's assertion, Klein did learn the facts to which he testified during the course of his employment. AOB 51-52.

The statements to Klein by his supervisor and AT&T management connecting the NSA to the copying and diversion of plaintiffs' communications to the SG3 room are admissible on multiple grounds. AOB 50-52. The district court did not exclude any of this evidence, finding only that the evidence was insufficient to establish that AT&T was the government's agent (ER 17, 19), and the government errs in asserting otherwise (GB 58, 60).

Contrary to the government's accusation of "bootstrapping" (GB 60), Federal Rule of Evidence 801(d) expressly permits these statements themselves to be used to establish that AT&T is the government's agent,

along with the independent evidence of AT&T's admission that it conducts FISA surveillance on behalf of the government (ER 911, 913), and the NSA Draft OIG Report's confirmation that AT&T conducts Internet content surveillance for the government (ER 121, 128, 1029-30).

Apart from their Rule 801(d) admissibility as agent-admissions, the statements by Klein's supervisor and AT&T management regarding meetings with the NSA are independently admissible under Federal Rule of Evidence 803(3) as statements of plan or intent. AOB 52-53. The government is incorrect in contending that the statements are only inadmissible statements of belief. GB 60-61.

In paragraph 16 of the Klein Declaration, Klein's supervisor "FSS#1 told [Klein] that another NSA agent would again visit . . . to talk to FSS#1." ER 1076. That is a direct statement by FSS#1 of his/her plan and intent to meet with the NSA agent. Paragraph 16 also includes a further statement that FSS#1's motive and plan for the meeting with the NSA agent was to discuss the suitability of employee FSS#3 taking over employee FSS#2's job of operating the secret SG3 room where plaintiffs' Internet communications were sent after being copied. *Id*.

Paragraph 10 contains a statement of intent by FSS#1 to receive a visit by an NSA agent on a different occasion at the facility FSS#1 managed, and a statement of FSS#1's plan and intent that the NSA agent should meet with FSS#2. ER 1075. It also contains a statement by AT&T higher

management that their plan and intent was for the NSA agent to visit the facility.

These statements are also evidence that the planned meetings with the NSA agents actually occurred.[10] AOB 48, 53.

Additionally, Klein himself testifies that NSA agents came to interview his coworkers. ER 1075-76. The government faults him for not expressly stating that he personally observed the agents (GB 59), but there was no need for him to do so. His declaration begins with an express assertion of personal knowledge. ER 1074. Personal knowledge can also be inferred from his statements. *Barthelemy v. Air Lines Pilots Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990). "Testimony should not be excluded for lack of personal knowledge unless no reasonable juror could believe that the witness had the ability and opportunity to perceive the event that he testifies about." *U.S. v. Hickey*, 917 F.2d 901, 904 (6th Cir. 1990).

Finally, Klein also has direct personal knowledge of the NSA's involvement with the SG3 room because he knows the only reason he was excluded from the SG3 room is because he had not been cleared by the NSA. ER 1076.

---

[10] The government also errs in asserting that these statements are not evidence that the persons with whom AT&T employees met actually were NSA agents (GB 60-61). In the seminal case of *Mutual Life Ins. Co. of New York v. Hillmon*, 145 U.S. 285, 296 (1892), a declarant's statement that he intended to depart with "X" was admitted to prove that he actually departed with X, and not with some other person he erroneously believed to be X.

b. The AT&T Documents And The Russell Declaration

The AT&T documents, authenticated both by Klein and by AT&T's hand-picked witness James Russell, are admissible as business records, as statements of plan or intent, and as statements of AT&T as the government's agent. AOB 45-49. In a convoluted exposition, the government tries but fails to demonstrate that Russell does not mean what he says when he attests from "personal knowledge" (ER 1197, ¶1) that AT&T's Folsom Street Facility contains the equipment described in the AT&T documents and in Klein's statements. GB 65.

The district court did not find that Russell lacked personal knowledge, as the government erroneously contends. GB 65. It said that Russell's statements were unreliable (ER 16)—an impermissible assessment of weight, not admissibility, and one that lacks any basis in the record, as AOB 45-46, 83-84 explains.

The government misdescribes the AT&T documents: Their author, Matthew Casamassima, is not an outside consultant as the government contends (GB 63) but an "AT&T employee" as Russell testifies and as Casamassima's "att.com" email address on the unredacted AT&T documents shows. ER 1203-04; ECF Nos. 84-3, 84-4, 84-5, 84-6. The documents themselves show that they are not a never-implemented proposal as the government contends (GB 64), for one page of the documents, ER 1280, lists the dates between January 22 and February 27, 2003 when

various stages of implementation were completed, making the documents contemporaneous with the conditions they record.[11] ER 1280 shows that the installation of the splitters to copy and divert to the SG3 room plaintiffs' communications as described in the documents actually occurred, and that the AT&T documents were current at the time of implementation.

The government's further objection (GB 64) that the copying and diversion of Internet backbone communications to the SG3 room shown by the documents is not a regularly conducted activity of AT&T's lacks merit, for Klein testifies that he conducted that activity continuously as part of his assigned duties. ER 1075-79.

Finally, the government makes an unsupported challenge to the accuracy of the AT&T documents. GB 64-65. It is the government's burden to show that the documents are untrustworthy (Fed. R. Evid. 803(6)(E)), but it has not put in any evidence calling into question the accuracy of anything stated in the documents. It ignores the testimony of Russell and Klein verifying that the equipment described in the AT&T documents is actually present in AT&T's Folsom Street Facility—testimony showing the trustworthiness of the documents that fully satisfies Federal Rule of Evidence 803(6) and *ABS Entm't, Inc. v. CBS Corp.*, 908 F.3d 405, 425-26 (9th Cir. 2018).

[11] This is yet another example of the government viewing the evidence in the light most favorable to itself, rather than plaintiffs.

2. Plaintiffs' Experts

The government repeats the district court's criticisms of plaintiffs' experts, but again these criticisms go to the weight, not the admissibility, of the expert testimony. The government put in no expert testimony of its own to counter plaintiffs' experts or demonstrate that their conclusions are not well founded.

The government (GB 61-62) wrongly labels as speculation expert Scott Marcus's carefully-considered conclusion that it was highly unlikely AT&T constructed for its own business purposes the surveillance apparatus shown in the AT&T documents and attested to by Russell and Klein, and highly probable that it did so to conduct government surveillance (ER 1043-46, 1065-69). But Marcus is not speculating, he is explaining what the equipment is designed to do. He has the expertise to draw his conclusions because he worked for years designing Internet backbones for telecommunications companies, provided Internet backbone services to AT&T, and was the FCC's Internet expert. ER 1037-40; AOB 53-54, 85-86. Indeed, what lacks any evidentiary foundation is the government's notion that AT&T acted with an innocent commercial purpose in copying and diverting its customers' communications to a secret room to which only a single employee with a government security clearance has access.

Expert Ashkan Soltani explains how the practices of Internet service providers increase the likelihood that the government's Internet backbone surveillance devices, wherever they might be located, would intercept

plaintiffs' communications. AOB 87. The government and the district court both make the fundamental error of claiming Soltani's testimony is inadmissible unless it can bear the entire burden of proving plaintiffs' case. GB 66; ER 17. But evidence is probative—and admissible—whenever, like Soltani's, it makes a fact of consequence more probable, regardless of how much more probable or whether standing alone it is sufficient to prove the fact. Fed. R. Evid. 401, 402.

C. The Public Evidence Shows Plaintiffs' Standing For Their Internet Metadata Claims

The government disparages the weight of plaintiffs' evidence showing the metadata of their Internet communications was intercepted. GB 49-53. But a reasonable factfinder considering all of the evidence could easily conclude it is more probable than not that plaintiffs' Internet metadata was collected. The NSA OIG Report establishes that AT&T was one of the companies providing Internet metadata to the government; the AT&T documents establish that the SG3 room contained a "Meta Data Cabinet"; the government's admissions establish that this massive program had an extremely broad authorized scope and in practice exceeded even those lax limits; plaintiffs' experts explain that Internet communications follow unpredictable paths across the Internet that are not predetermined (e.g., "There is potential for any traffic to pass through any node," ER 974), and so are likely to encounter the government's surveillance devices wherever they are located. AOB 55-58.

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

As the AOB explains, plaintiffs are entitled to partial summary judgment on their Fourth Amendment Upstream Internet interception claim because the undisputed evidence shows their Fourth Amendment rights have been violated. AOB 64-79.

The government wrongly seeks to foreclose the Court from considering the merits of plaintiffs' Fourth Amendment Upstream Internet interception claim by refusing to contest the claim on appeal. But an appellee cannot foreclose this Court's review of a summary judgment denial simply by waiving the opportunity to argue the issue on appeal.

The Fourth Amendment Internet interception claim is before the Court after final judgment with an extensive evidentiary record and the Court should decide it. Below, plaintiffs and the government fully joined issue, filing cross-motions for summary judgment on plaintiffs' Fourth Amendment Internet interception claim. ECF Nos. 261, 285, 294, 299. Plaintiffs and the government both presented extensive evidence and argument contesting the merits of whether the government's Upstream Internet interception violated the Fourth Amendment. ECF Nos. 262 to 265, 288, 295, 300. Proceedings spanned seven months from initial briefing to decision.

There is nothing "piecemeal" about reviewing the Fourth Amendment claim now before the Court. Indeed, the government obtained dismissal of

plaintiffs' previous Rule 54(b) appeal from the Fourth Amendment ruling on the ground that it should be reviewed on appeal from a final judgment on all of plaintiffs' claims. That time has now arrived.

Remanding the issue without deciding it, as the government suggests, would thwart the interests of justice. The government surveillance issues raised by this lawsuit remain current and vital, not just for plaintiffs but for all Americans. Yet plaintiffs have already been forced to wait over a decade to have them adjudicated. Further delay is untenable. If the Court were to remand the issue, it would result in yet another round of summary judgment proceedings in the district court that would eventually and inevitably end up being appealed years later to this Court by the losing party. At that time, the issue before the Court would be exactly the same as it is now.

The government, of course, would prefer that the day of judgment be postponed indefinitely. Already, the government has spoliated evidence. ECF No. 386-2. As time passes, more evidence will be lost as documents are destroyed, memories fade, and witnesses and defendants die. One plaintiff, too, has died while this case has been pending. The "just, speedy, and inexpensive" determination of this claim is best served by the Court deciding now whether the record entitles plaintiffs to summary judgment on their Fourth Amendment Internet interception claim. Fed. R. Civ. P. 1.

The constitutional avoidance doctrine, glancingly referenced by the government, also provides no basis for avoiding a decision. That doctrine applies only where a lawsuit can be fully resolved on nonconstitutional

grounds. That is not the case here. This lawsuit cannot be fully resolved without deciding the Fourth Amendment issue. Plaintiffs seek an injunction prohibiting the Internet interception practices they challenge, and only their Fourth Amendment claim can provide an injunction. Plaintiffs' statutory Internet interception claims are limited to damages relief. § 2712(d).

V. Other Issues

A. The Court Must Review The Secret Evidence And The District Court's Secret Opinion

The Court should reject the government's suggestion that in deciding the appeal the Court should not look at the secret evidence or the district court's secret opinion. GB 15. The Court's review must be based on the full record below, including the secret evidence and the district court's secret opinion. The Court's review of the secret evidence will undoubtedly confirm that plaintiffs have standing and are aggrieved persons.

Because plaintiffs have been denied access to the secret evidence, they have not been able to present it to the Court as they would ordinarily do in their role as appellants. Thus, as a matter of due process, the Court must review the secret evidence to determine whether it supports plaintiffs' standing and aggrieved-person status. For the reasons explained above and at AOB 58-60, the secret evidence as well as the public evidence may be used to establish plaintiffs' standing and aggrieved-person status. Like the public evidence, the secret evidence must be viewed holistically and in the light most favorable to plaintiffs.

The Court should also review the district court's secret opinion, even though review of the issues is de novo and the district court's holdings are not subject to any deference by this Court. The secret opinion is part of the district court's dispositive ruling, and should be reviewed just as the Court always reviews a district court's complete ruling, even when the Court decides the issues de novo. The secret opinion "review[s] and adjudicate[s] the effect of the classified evidence regarding Plaintiffs' standing to sue." ER 15.

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

The government argues that plaintiffs should not be granted access to the classified evidence on the ground that the plaintiff-access procedures of section 1806(f) have never previously been used. GB 67-69. The Court should reject this argument. Congress enacted the plaintiff-access procedures of section 1806(f) intending them to be used in appropriate cases. There will never be a more appropriate case than this one, challenging the unlawful mass surveillance of millions of Americans.

That the government further faults plaintiffs for not demonstrating in detail how the lack of access has hampered their case only proves plaintiffs' point: Without access to the secret evidence, plaintiffs have no notice of it and no opportunity to use it to support their claims, to rebut the government's defenses, or otherwise respond to it.

Finally, the government contends that when it triggered section 1806(f)'s procedures by asserting that national-security information was at issue, that caused plaintiffs to lose their right to due process (GB 69), but that is not how section 1806(f) or the due process clause work.

C. Plaintiffs' Claims Are Redressable

The government makes no attempt to defend the district court's erroneous ruling that plaintiffs' claims are not redressable, and thus that is not a ground on which the judgment can be affirmed. AOB 62-64.

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

The appellees make no separate argument regarding the personal-capacity defendants, and thus the judgment must be reversed as to them too. AOB 64.

CONCLUSION

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

Dated: January 27, 2020

Respectfully submitted,

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

CINDY A. COHN

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

THOMAS E. MOORE III
ROYSE LAW FIRM

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

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs-Appellants

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

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

I am the attorney or self-represented party.

This brief contains 9,890 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

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

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

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

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

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

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

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

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

Signature: ___*s/Richard R. Wiebe*_____ **Date:** January 27, 2020