No. 19-16066

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CAROLYN JEWEL, et al.,

Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, et al.,

Defendants-Appellees.

On Appeal from the United States District Court
for the Northern District of California

BRIEF FOR APPELLEES

JOSEPH H. HUNT
Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

H. THOMAS BYRON III
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes:

Rules:

Legislative Material:

Other Authority:

INTRODUCTION

In order to maintain their suit challenging alleged government surveillance, plaintiffs must put forward admissible evidence supporting standing—that is, evidence supporting their allegations that their communications (or metadata about those communications) have been subject to the intelligence-collection activities they seek to challenge. The district court carefully reviewed plaintiffs' proffered evidence and correctly concluded that some should be excluded on evidentiary grounds, and the remaining evidence was insufficient to withstand summary judgment.

Plaintiffs chiefly contend on appeal that the district court should have looked beyond the evidence they submitted, and instead should have determined standing based on classified and privileged information submitted by the government *ex parte* and *in camera*. But the district court held—and plaintiffs do not dispute in this appeal—that rendering a decision on standing by using classified information submitted by the government "would jeopardize the national security" and reveal state secrets. ER 27. Where the state-secrets privilege has been properly invoked and upheld by the district court, privileged evidence is "completely removed from the case," and, if necessary, the case is dismissed if "litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1081-83 (9th Cir. 2010) (en banc).

Plaintiffs cannot avoid those effects of the state-secrets privilege by pointing to a procedure described in a provision of the Foreign Intelligence Surveillance Act of

1978 (FISA), 50 U.S.C. § 1806(f), for *ex parte* and *in camera* review of certain information. Even if Section 1806(f), in the narrow circumstances where it applies, were to displace the state-secrets privilege to determine the "legality" of electronic surveillance, *see Fazaga v. FBI*, 916 F.3d 1202, 1230-34 (9th Cir. 2019), it does not enable courts to determine whether plaintiffs were subject to electronic surveillance in the first place, much less to do so using privileged information whose disclosure would damage national security. Nor does the statute relieve plaintiffs of their burden of supporting standing with admissible evidence, or shift that burden to the government to support or disprove standing with *in camera* submissions—a procedure that the Supreme Court has expressly rejected. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 412 n.4 (2013). The judgment of the district court should be affirmed.

STATEMENT OF JURISDICTION

Plaintiffs' complaint invoked the district court's jurisdiction under 28 U.S.C. § 1331. ER 1101. The district court granted the government's motion for summary judgment and entered final judgment as to all claims on April 25, 2019. ER 1. Plaintiffs filed a timely notice of appeal on May 20, 2019. ER 82-83; *see* Fed. R. App. P. 4(a)(1)(B). This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

The questions presented are:

1. Whether the district court correctly held that FISA's *ex parte* and *in camera* procedures for judicial determination of the "legality" of electronic surveillance do not

relieve plaintiffs of their burden to establish, using non-privileged evidence, the threshold questions of standing and "aggrieved-person" status; and

2. Whether the district court correctly held that plaintiffs failed to introduce admissible evidence supporting standing.

PERTINENT STATUTES AND REGULATIONS

Pertinent statutes are reproduced in the addendum to this brief.

STATEMENT OF THE CASE

Plaintiffs filed this case in district court in 2008, seeking to challenge what they alleged to be indiscriminate, dragnet surveillance of internet and telephone communications (and related metadata) conducted by the National Security Agency (NSA), allegedly in violation of several statutory and constitutional provisions. After many years of litigation, the district court ultimately dismissed all plaintiffs' claims on summary judgment for lack of standing and because further litigation regarding standing would threaten to reveal information protected by the state-secrets privilege.

A. Factual and Legal Background

1. NSA Intelligence-Gathering Programs

In the wake of the terrorist attacks of September 11, 2001, in order to detect and thwart additional attacks, President Bush authorized the NSA to conduct three intelligence-gathering programs, known collectively as the President's Surveillance Program. The Program involved (1) the targeted collection of the content of certain communications reasonably believed to involve agents of al-Qaida or other terrorist

organizations; (2) the bulk (*i.e.*, non-targeted) acquisition of call-detail records, or metadata about telephone calls made to, from, or within the United States, such as dates, times, durations, and originating and receiving numbers; and (3) the bulk (non-targeted) collection of metadata about internet-based communications, such as the dates, senders, and recipients of email. *See* SER 41-42, 59-60, 66 (Decl. of then-NSA Dir. Rogers) (public version).

The President's Surveillance Program has been discontinued. By early 2007, the three activities described above had transitioned to programs authorized under various provisions of FISA and supervised by the Foreign Intelligence Surveillance Court (FISC). SER 59-60. So-called "upstream" collection, for example, selectively collects the content of certain internet communications (such as emails) associated with targeted "selectors" (such as an email address associated with a terrorist abroad) as those communications transit the "Internet backbone." ER 433-34 (report of the Privacy and Civil Liberties Oversight Board); *see* SER 44-45, 51-54 (Rogers Decl.). Such collection is conducted pursuant to FISA Section 702, which creates a court-authorized mechanism whereby the government may "target[] … persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a).

In addition to this ongoing targeted collection of the content of certain internet communications of non-U.S. persons located abroad, NSA used to, but no longer does, collect certain bulk metadata under FISA—though it never captured "all (or

virtually all)" such metadata. SER 55 (Rogers Decl.). From 2006 to 2015, the NSA acquired certain bulk metadata about (but not the content of) telephone calls under 50 U.S.C. § 1861(a)(1). *See* SER 54-57, 59-60; SER 7 (Decl. of then-Principal Deputy Dir. of Nat'l Intelligence Susan Gordon). And, between 2004 and 2011, the NSA collected certain bulk metadata about (but not the content of) internet communications under 50 U.S.C. § 1842(a)(1). *See* SER 58-60 (Rogers Decl.); SER 7 (Gordon Decl.). Both of these FISA-authorized programs have been discontinued, and the relevant provisions of FISA have been amended to permit only targeted collection using "specific selection term[s]." 50 U.S.C. § 1861(b)(2)(C); *id.* § 1842(c)(3); *see* SER 46-48 (Rogers Decl.).

The government has publicly acknowledged the existence of these intelligence-gathering activities and declassified certain information about their operation to "promot[e] informed public debate about the value and appropriateness of these programs." SER 5 (Gordon Decl.). But specific operational details—including the targets and subjects of surveillance, the providers that have assisted the NSA, and technical details about what information has been collected, and how—remain classified. SER 9; SER 60, 89-90 (Rogers Decl.). Disclosing such operational details publicly "would cause exceptionally grave damage to the national security of the United States," as such disclosures would, for example, "tend to reveal to our enemies who are the NSA's actual targets of surveillance and who are not, which channels of communication are free from NSA surveillance and which are not, and perhaps also

sensitive intelligence methods and sources," and such revelations would "help our adversaries evade detection and capitalize on limitations in the NSA's surveillance capabilities." SER 28, 31 (Rogers Decl.); *see* SER 94-96; SER 10-15 (Gordon Decl.).

2. The State-Secrets Privilege

"The Supreme Court has long recognized that in exceptional circumstances courts must act in the interest of the country's national security to prevent disclosure of state secrets, even to the point of dismissing a case entirely." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc). The longstanding state-secrets privilege may be invoked over certain information the disclosure of which could "expose military [or state-secret] matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 10 (1953).

Where the privilege has been invoked by the head of the Executive Branch department with control over the information, and a court rules that there is a "reasonable danger" that disclosing the information would threaten the national security, the information "is completely removed from the case." *Jeppesen Dataplan*, 614 F.3d at 1081-82. The case may then proceed "with no consequences save those resulting from the loss of evidence." *Id.* at 1082. Dismissal is required, however, where the case cannot proceed—such as where a plaintiff cannot continue to litigate a matter using the remaining information, where the loss of information deprives the defendant of a "valid defense," or where litigation using the remaining information would pose an unacceptable risk of disclosing privileged information. *Id.* at 1083.

3. The Foreign Intelligence Surveillance Act

FISA regulates how the government conducts electronic surveillance for foreign-intelligence purposes, and, as relevant here, it regulates how the government uses information obtained or derived from such surveillance. *See* 50 U.S.C. § 1806. If the government "intends to enter into evidence or otherwise use or disclose in any … proceeding … , against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person," the government must "notify the aggrieved person" and the tribunal. *Id.* § 1806(c)-(d). An aggrieved "person against whom" the evidence would be used may "move to suppress the evidence … on the grounds that" it was "unlawfully acquired" or "the surveillance was not made in conformity with an order of authorization." *Id.* § 1806(e).

In those circumstances—that is, after government notification, a suppression motion, or a similar motion by an "aggrieved person"—FISA establishes procedures for a judicial determination of "the legality of the surveillance" that produced the information or evidence. 50 U.S.C. § 1806(f). Where Section 1806(f) applies, if the Attorney General attests that "disclosure or an adversary hearing would harm the national security," the district court must review the underlying applications, orders, and related materials *ex parte* and *in camera* to determine "the legality of the surveillance." *Id.* If the court "determines that the surveillance was not lawfully authorized or conducted, it shall … suppress the evidence … or otherwise grant the motion of the aggrieved person." *Id.* § 1806(g).

A panel of this Court recently held in *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), that, in certain circumstances, Section 1806(f)'s *in camera* and *ex parte* procedures displace the state-secrets privilege and allow for judicial determination of the lawfulness of electronic surveillance based on the court's *ex parte* and *in camera* examination of privileged information that would otherwise be removed from the case. *Id.* at 1230-34. The *Fazaga* panel also concluded that Section 1806(f)'s procedures would apply in that case. The panel reasoned that the government's assertion of the state-secrets privilege amounted to an assertion that "the Government would like to use this information to defend itself," equating the removal of privileged evidence from a case to notice under Section 1806(c) of the government's intent to "use" the results of electronic surveillance "against an aggrieved person." *Id.* at 1235. The government disagrees with those conclusions and has sought rehearing.

B. Prior Proceedings

1. Plaintiffs are five individuals (one since deceased) residing in California who use or used telephone and internet services provided by (among others) AT&T or Verizon. ER 1102 (compl.), ER 999-1024 (affidavits). Plaintiffs brought this action in 2008, alleging that the government has engaged in "dragnet" surveillance since October 2001. ER 1099 (compl.).[1]

[1] Plaintiffs brought this putative class action against the United States, several government agencies, and certain federal officials; the complaint also named a number of former officials in their personal capacities. ER 1103-04. The final order disposing

Relying primarily on allegations about what was happening in 2003 inside a room at an AT&T facility in San Francisco, ER 1106-10, plaintiffs allege that the government captures the content of their internet communications using a "network of sophisticated communications surveillance devices, attached to the key facilities of telecommunications companies such as AT&T that carry Americans' Internet … communications." ER 1100. Plaintiffs also allege that the government obtains metadata about their communications—"records indicating who the customers communicated with, when and for how long"—from "telecommunications companies such as AT&T." ER 1100.

Plaintiffs contend that the alleged surveillance violates, as relevant here, the Fourth Amendment, the Wiretap Act, *see* 18 U.S.C. § 2511(a), (c), (d), and the Stored Communications Act, *see* 18 U.S.C. § 2703(a)-(c).[2]

2. After protracted proceedings over many years, including two prior appeals to this Court, the district court ultimately granted the government's motion for summary judgment as to all claims, holding that further litigation about standing was precluded by the state-secrets privilege, and further holding that plaintiffs failed to

---

of all of plaintiffs' claims against the government also resolved "all personal-capacity claims" on the same grounds. ER 27. This brief is filed on behalf of all defendants, including the personal-capacity defendants.

[2] Plaintiffs affirmatively abandoned their other constitutional claims against the government. *See* Joint Case Management Conf. Statement 2, ECF 352 (May 5, 2017). And they do not challenge in this appeal the district court's dismissal of their other statutory claims against the government. *See* ER 70-79.

support standing with admissible evidence on the public record. ER 3-26. The court rejected plaintiffs' motion to adjudicate standing on the basis of privileged evidence using FISA's *ex parte* and *in camera* procedures. ER 25-27.

a. At the outset, the district court had dismissed all of plaintiffs' claims for lack of standing at the pleading stage, and this Court reversed, concluding that plaintiffs' allegations of dragnet surveillance were sufficient, if true, to establish standing, and further holding that, at the pleading stage, those allegations must be "accept[ed] as true." *Jewel v. NSA*, 673 F.3d 902, 910-11 (9th Cir. 2011).

On remand, the district court, while disposing of several statutory claims no longer at issue in this case, held that FISA's *ex parte* and *in camera* procedures, 50 U.S.C. § 1806(f), "displace[] the state secrets privilege" with respect to adjudication of the legality of electronic surveillance. ER 67. And the district court determined that Section 1806(f)'s procedures could apply to determine the merits of plaintiffs' remaining Wiretap Act and Stored Communications Act claims for damages against the government. *Id.*; *see* 18 U.S.C. § 2712(b)(4) (providing that "the procedures set forth in" Section 1806(f) "shall be the exclusive means by which materials governed by [Section 1806(f)] may be reviewed" in an action against the United States for damages under those Acts). But the district court warned that, even where Section 1806(f) "provides the mechanism for review of submitted materials, Plaintiffs shall be tasked with the burden to establish standing to sue without resulting in impermissible

damage to ongoing national security efforts." ER 79 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 412 n.4 (2013)).

b. The district court granted partial summary judgment to the government on the Fourth Amendment challenge to targeted collection of certain internet content. ER 46-55. The court held that "the evidence at summary judgment is insufficient to establish that the Upstream collection process operates" as a dragnet capturing all communications, including plaintiffs', transiting AT&T facilities. ER 52. The court also held that "whether Plaintiffs have standing … cannot be litigated without impinging" on information protected by the state-secrets privilege regarding operational details of upstream collection, and that dismissal was therefore required. ER 54. This Court dismissed plaintiffs' interlocutory appeal from that decision, noting that the district court's reasoning "cannot be limited to the narrow Fourth Amendment claim" and "raised a potential standing bar for *all* claims." *Jewel v. NSA*, 810 F.3d 622, 630 (9th Cir. 2015) (emphasis added).

c. On remand, the district court ordered the government to respond to plaintiffs' jurisdictional discovery requests regarding standing for their remaining statutory claims. ER 34. The district court also separately ordered the government to "marshal all … evidence relating to Plaintiffs' standing," and to "present that evidence to the Court … *ex parte* and *in camera*" while making available on the public docket any unclassified and unprivileged material. ER 34.

The government did not concede that the order to submit voluminous and extraordinarily sensitive information about state secrets for *ex parte* and *in camera* inspection was appropriate. *See Reynolds*, 345 U.S. at 10 (warning that, where doing so is not necessary to determine that the state-secrets privilege applies, "the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers"); *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005) ("Courts are not required to play with fire.").

The government nonetheless complied, filing, *ex parte* and *in camera*, a 193-page declaration by then-NSA Director Michael Rogers. *See* SER 18-108 (redacted public version). The declaration "compiles and presents, in expansive detail, (i) information as to whether Plaintiffs' communications (or metadata associated with them) have been subjected to the challenged NSA intelligence-gathering activities, (ii) information concerning the sources, methods, and technical operational details of the challenged activities, so far as it provides circumstantial evidence regarding Plaintiffs' standing, and (iii) information concerning whether Plaintiffs' telecommunications service providers have provided assistance to the NSA in conducting these programs." SER 28. The declaration also explained in greater detail, and in classified terms, the specific harm that disclosure of the privileged information would have on the national security. *See* SER 91-107 (¶¶ 324-84). The government also filed, *ex parte* and *in camera*, "thousands of pages" of underlying, highly classified documents supporting the declaration. Tr. 58, ECF 461 (Apr. 5, 2019).

In addition to extensive and detailed classified information submitted to the district court for *ex parte* and *in camera* review, the government filed on the public docket the declaration of then-Principal Deputy Director of National Intelligence Susan Gordon. *See* SER 1-15. That declaration explained, in as much detail as possible in an unclassified setting, why confirming or denying plaintiffs' standing, or related operational details about NSA's intelligence-gathering activities, "reasonably could be expected to cause exceptionally grave damage to the national security of the United States" by, for example, revealing to our adversaries which channels of communication are free from NSA surveillance and which are not. SER 4, 10-15. The declaration invoked the state-secrets privilege over that information.[3]

The government also objected to plaintiffs' discovery requests. *See* ECF 388-1 (Feb. 16, 2018). In compliance with the district court's order to "marshal all evidence" for the court's *in camera* review, the government did "not with[o]ld any information" from the *ex parte* and *in camera* submissions "on the basis of the[se] objections." *Id.* at 11. The government also provided on the public docket any responses to plaintiffs' discovery requests that sought unprivileged and unclassified information relevant to standing. *E.g. id.* at 37-38.

d. The district court granted the government's motion for summary judgment on the remaining statutory claims for lack of standing and because further

[3] The government also invoked two statutory privileges, 50 U.S.C. §§ 3024(i)(1), 3605(a), *see* SER 9; SER 107, though the district court ultimately did not address them.

adjudication of plaintiffs' standing would reveal state secrets. ER 3-28. After evaluating all of plaintiffs' evidence, the court concluded that plaintiffs "failed to proffer sufficient admissible evidence to indicate that" their communications had been subject to the alleged surveillance. ER 20.

The district court upheld the government's invocation of the state-secrets privilege over the information submitted *ex parte* and *in camera*, concluding that "there is a reasonable danger the disclosure of the information at issue here would be harmful to national security." ER 23. Plaintiffs do not challenge that determination in this appeal. The district court also rejected plaintiffs' argument that the court must nevertheless use FISA's *ex parte* and *in camera* procedures to determine plaintiffs' standing based on privileged information. ER 25. The court explained that its prior order, and *Fazaga*, had held only that those procedures displace the state-secrets privilege and are "to be used when 'aggrieved persons' challenge the *legality* of electronic surveillance," and that a court's *ex parte* and *in camera* review of evidence under those procedures is available only "'to determine whether the electronic surveillance was lawfully authorized and conducted.'" ER 25 (emphasis added) (quoting *Fazaga*, 916 F.3d at 1238, 1252). The court explained that *Fazaga* did not address "what to do when, as here, the answer to the question whether a particular plaintiff was subjected to surveillance … is the very information over which the Government seeks to assert the state secrets privilege." ER 25. In those circumstances, the district court held, plaintiffs may not invoke FISA procedures to

help meet their burden of establishing standing or status as "aggrieved persons" "where the very issue of standing implicates state secrets." ER 25-26.

The district court also carefully reviewed all of the material in the record, including classified and privileged information submitted *ex parte* and *in camera*. ER 26. Based on that information, the court determined that further litigation would pose a risk of disclosing privileged national-security information. The court recognized that "even a simple 'yea or nay' as to whether Plaintiffs have standing to proceed on their statutory claims would do grave harm to national security." ER 26. For that reason and "because a fair and full adjudication … would require potentially harmful disclosures of national security information that are protected by the state secrets privilege," the court concluded that "permitting further proceedings would jeopardize the national security." ER 27.

The district court also issued a classified opinion reviewing the information over which the government claimed privilege and explaining in more detail why removal of that information and dismissal of the case was appropriate to protect national security. That classified opinion, like the government's *ex parte* and *in camera* submissions, is available to this Court for review *ex parte* and *in camera*, although resolution of the issues presented in this appeal does not require such review.

SUMMARY OF ARGUMENT

The district court correctly resolved the few remaining issues in this long-running case. As the district court correctly held (and as plaintiffs do not dispute),

further adjudication of whether plaintiffs were subject to the intelligence-gathering activities that they seek to challenge would reveal state secrets. The district court thus correctly granted summary judgment because plaintiffs cannot establish standing.

On appeal, plaintiffs chiefly contend that the district court was required to determine standing using privileged evidence—even if doing so exposes state secrets and threatens the national security—because of a provision in FISA that creates *ex parte* and *in camera* procedures for determining "the legality of [electronic] surveillance" in certain circumstances. 50 U.S.C. § 1806(f). But, as that provision's plain text and purpose make clear, Section 1806(f) is not a vehicle for determining whether electronic surveillance has occurred in the first place. Plaintiffs must make that showing in order to support Article III standing. And they must make at least the same showing in order to use Section 1806(f)'s procedures. Being an "aggrieved person" whose communications were subject to electronic surveillance is among the statutory *preconditions* to successful invocation of Section 1806(f), not a matter to be addressed *using* Section 1806(f). Both standing and aggrieved-person status are thus threshold matters that plaintiffs must establish on their own using the normal modes of civil litigation. Those threshold requirements ensure that the statute does not create an open invitation for any plaintiff who chooses to file a lawsuit to automatically learn whether or not he or she has been subject to government surveillance. Plaintiffs failed to satisfy those threshold requirements, and further adjudication of those requirements is precluded by the state-secrets privilege. Thus,

even if Section 1806(f) were to displace the dismissal remedy of the state-secrets privilege by providing for *ex parte* and *in camera* determination of the "legality" of proven electronic surveillance, that principle has no application here, where plaintiffs have not established aggrieved-person status or standing. Plaintiffs cannot meet those threshold requirements using Section 1806(f) or privileged information.

This appeal can be resolved on those grounds. As the district court correctly held, and as plaintiffs do not dispute, the state-secrets privilege warranted dismissal of plaintiffs' claims because continued adjudication and dispositive determination of whether plaintiffs were subject to alleged intelligence gathering "would jeopardize the national security" by "requir[ing] potentially harmful disclosures of national security information that are protected by the state secrets privilege." ER 27. Plaintiffs' only argument on appeal regarding the state-secrets privilege is the erroneous two-part assertion that Section 1806(f) helps determine aggrieved-person status and standing and also displaces the state-secrets privilege for that purpose. Because they are wrong on both scores—and even if they were wrong on either—there is no need to address the myriad evidentiary issues plaintiffs raise on appeal. In any event, the district court did not abuse its discretion in resolving those evidentiary disputes. And plaintiffs were unable to identify admissible evidence indicating that their communications (or metadata about their communications) have been or will be subject to alleged intelligence gathering. Plaintiffs have thus failed to meet their burden under Article III, and the district court correctly granted summary judgment on all of their claims.

STANDARD OF REVIEW

This Court reviews summary judgment "de novo" and "evidentiary rulings for abuse of discretion." *Kaffaga v. Estate of Steinbeck*, 938 F.3d 1006, 1013 (9th Cir. 2019).

ARGUMENT

I. FISA's Procedures for Determining the Legality of Electronic Surveillance Do Not Relieve Plaintiffs of Their Obligation to Establish Standing Using Non-Privileged Evidence.

The district court correctly upheld the government's invocation of the state-secrets privilege over extremely sensitive details about classified NSA intelligence-gathering activities. As the government explained when invoking the privilege, it "would cause exceptionally grave damage to the national security of the United States" to publicly reveal "information concerning the sources, methods, and technical operational details" of NSA intelligence-gathering activities, including whether plaintiffs' "telecommunications service providers have provided assistance to the NSA in conducting these programs," and whether "[p]laintiffs' communications (or metadata associated with them) have been subjected to the challenged NSA intelligence-gathering activities." SER 28-29, 31 (Rogers Decl.). The district court independently reviewed the government's submissions, determined that revealing such operational details "would jeopardize the national security," and upheld the government's invocation of the state-secrets privilege. ER 23, 27.

As the district court correctly recognized, ER 27, under this Court's precedents applying the state-secrets privilege, the privileged information is "completely removed

from the case" in order to protect the national security. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1081-82 (9th Cir. 2010) (en banc). Once the privileged information is removed, the district court must determine whether further adjudication of standing would threaten to reveal state secrets, and thus risk harm to national security. *Id.* Here, as the court properly concluded, ER 27, dismissal is required on that basis. And, if dismissal were not independently required, plaintiffs would still be required to support standing using non-privileged evidence.

Plaintiffs do not dispute those effects of the state-secrets privilege, and they do not dispute that the government satisfied the procedural and substantive requirements to assert the privilege. Plaintiffs instead assert that the privilege has no application here. They contend that, irrespective of the risk of exceptionally grave damage to the national security, the district court was nevertheless required to disregard the privilege and to assess plaintiffs' standing using evidence regarding operational details of the NSA's intelligence-gathering activities, because of (A) a statute, 50 U.S.C. § 1806(f), and (B) the recent opinion of a panel of this Court in *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), interpreting that statute. *See* Br. 14-24. But neither the statute nor *Fazaga* require that perverse result, as the district court correctly held.

A. FISA Does Not Help Plaintiffs Establish Standing.

By its plain text, FISA's *ex parte* and *in camera* procedures in Section 1806(f) apply only to determine the legality of electronic surveillance in certain enumerated circumstances. Those procedures do not apply to determine the predicate factual

question whether electronic surveillance has occurred. Section 1806(f) is thus not an open invitation for any plaintiff who chooses to file a lawsuit to learn whether or not he or she has been subject to electronic surveillance. And, even if Section 1806(f)'s procedures were thought to apply to determine those threshold issues, it would not thereby displace the state-secrets privilege in that application.

1. Section 1806(f)'s *in camera* and *ex parte* procedures apply only in narrowly defined circumstances, such as when the government provides notice of its intent to "use" evidence derived from electronic surveillance "against" an "aggrieved person" in a proceeding, or when an "aggrieved person" files a motion to suppress, or similar motion, and thereby challenges the lawfulness of the surveillance. *See* 50 U.S.C. § 1806(c), (e), (f). In such circumstances, the Attorney General may then invoke the protections of Section 1806(f) by attesting that "disclosure or an adversary hearing would harm the national security of the United States." *Id.* § 1806(f).

And, to protect against that harm to national security, FISA provides that, "notwithstanding any other law" that may give the "aggrieved person" rights to access the information, the district court "review[s] *in camera* and *ex parte*" certain "materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). If, after this review, the court "determines that the surveillance was not lawfully authorized or conducted," then the court shall "suppress the evidence … or otherwise grant the motion of the aggrieved person." *Id.* § 1806(g).

2. Section 1806(f) is not a self-opening door. As its plain text makes clear, its procedures for reviewing information *in camera* and *ex parte* apply only in connection with a district court's determination of the "legality" and "lawful[ness]" of electronic surveillance, and only in narrowly circumscribed conditions, such as where the government gives notice of its intent to "use" evidence obtained or derived from electronic surveillance in a proceeding against an "aggrieved person," or an "aggrieved person" moves to suppress evidence or files a similar motion, and the government in fact invokes the protections of Section 1806(f). Nothing in the text of the statute suggests that a district court shall also use Section 1806(f) to help plaintiffs make the predicate *factual* showing that they were subject to surveillance in the first place where, as here, the government has *not* provided notice of such surveillance.

Congress knows how to create a procedure to compel the government to "affirm or deny" whether a person was subject to certain types of surveillance. 18 U.S.C. § 3504(a)(1). This "affirm or deny" procedure has no application here (plaintiffs do not contend otherwise). And, crucially, FISA includes no similar language that could conceivably compel the government to "affirm or deny" whether an act occurred. Congress instead carefully tailored Section 1806(f) to serve a different, and limited, purpose: to provide an avenue for determining "the *legality* of the surveillance" in certain enumerated circumstances, while avoiding the disclosure of classified and privileged information, such as, here, whether plaintiffs have been subject to surveillance. 50 U.S.C. § 1806(f) (emphasis added).

Similarly telling is Congress's definition of *whose* legal contentions may be resolved using Section 1806(f) procedures: an "aggrieved person." The statute defines an "aggrieved person" as "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) (emphasis added)—not someone who merely *asserts* such surveillance. This Court acknowledged as much in *United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987), where this Court explained that whether a person is "aggrieved" is "a threshold matter" to be determined *before* Section 1806(f)'s procedures are used to determine the lawfulness of surveillance. *Id.* at 789.[4]

That threshold aggrieved-person requirement is in keeping with Congress's overall design of Section 1806(f)'s procedures to avoid damaging public disclosures of classified and privileged information. For example, Congress explained that, if the government seeks to prosecute a defendant using evidence derived from electronic surveillance under FISA, if the defendant seeks access to materials related to the surveillance, and if the court determines that such access would be necessary to help the court determine the legality of the surveillance, the government nonetheless can prevent such disclosure by simply "choos[ing]" to "forgo the use of the surveillance-

[4] Contrary to plaintiffs' contentions, Br. 25, this "threshold" requirement for invoking Section 1806(f) is consistent with this Court's description, in the first appeal in this case, of aggrieved-person status as not involving Article III jurisdiction but rather "a merits determination" to be made by applying the statutory definition of who qualifies as an "aggrieved person." *Jewel*, 673 F.3d at 907 n.4.

based evidence" in the prosecution and thereby avoid the risk that Section 1806(f)'s procedures "would damage the national security." S. Rep. No. 95-701, at 65 (1978).

3. Disregarding this plain text and purpose, plaintiffs contend that Section 1806(f), far from *avoiding* damaging public disclosures, actually *facilitates* such disclosures. They argue that Section 1806(f) allows anyone to compel the government to disclose whether he or she has been subject to electronic surveillance merely by filing a complaint alleging that such surveillance has taken place. At that point, plaintiffs say, they can force the government to submit, and the court to render a decision based on, state-secrets evidence regarding standing and aggrieved-person status. *See* Br. 22 ("[N]o evidentiary showing is required.").

But the Supreme Court considered and rejected precisely that kind of *ex parte* and *in camera* procedure to establish standing to challenge electronic surveillance in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). There, plaintiffs failed to introduce sufficient evidence on the public record on summary judgment to support standing. A suggestion had been made at oral argument "that the Government could help resolve the standing inquiry by disclosing to a court, perhaps through an *in camera* proceeding … whether it is intercepting [the plaintiffs'] communications," but the Court rejected that suggestion as "puzzling." *Id.* at 412 n.4. "[I]t is [the plaintiffs'] burden to prove their standing by pointing to specific facts, … not the Government's burden to disprove standing by revealing details of its surveillance priorities." *Id.*

Moreover, the Court recognized the obvious mischief created by a procedure requiring the government to confirm or deny surveillance: It "would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program." *Clapper*, 568 U.S. at 412 n.4. The court's "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.* The Court understandably rejected the invitation to create an *in camera* procedure with that kind of grave consequence.

It is thus unsurprising that Congress, too, declined to turn Section 1806(f) into a vehicle for forcing the government to confirm or deny highly classified operational details of NSA intelligence-gathering activities. The D.C. Circuit, in analyzing this question, recognized the stakes: "[I]f the government is forced to admit or deny such allegations" of electronic surveillance, it "will have disclosed sensitive information that may compromise critical foreign intelligence activities." *ACLU Found. of S. California v. Barr*, 952 F.2d 457, 468 & n.13 (D.C. Cir. 1991). Based on those concerns, and the statute's text and purpose, the D.C. Circuit correctly interpreted Section 1806 as not creating a "duty to reveal ongoing foreign intelligence surveillance." *Id.* at 468 n.13. The court held that, in a summary judgment motion to dismiss claims challenging alleged surveillance, "[t]he government would need only assert that plaintiffs do not have sufficient evidence to carry their burden of proving ongoing surveillance," and that, "[i]f plaintiffs are ultimately unable to come forward with such evidence, the

district court must conclude that there is no 'genuine' dispute about these material facts and enter summary judgment in favor of the government." *Id.* at 469.

So, too, here. Section "1806(f) procedures do not apply where, as here, the plaintiff has merely plausibly alleged that it has been the target of surveillance and has not yet adduced evidence establishing this fact of surveillance." *Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 786 (D. Md. 2018).

B. This Court's Precedent Reinforces that Conclusion.

As the district court correctly recognized, the recent panel opinion of this Court in *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), further confirms that Section 1806(f) does not relieve plaintiffs of their burden to establish standing and aggrieved-person status using nonprivileged evidence.

1. The *Fazaga* plaintiffs alleged that the FBI had conducted an investigation (including alleged electronic surveillance) in violation of various statutory and constitutional provisions. 916 F.3d at 1214. The government invoked the state-secrets privilege over national-security information, including whether particular sources and methods (including electronic surveillance) were used. *Id.* at 1215.

Fazaga held, on a motion to dismiss where the alleged surveillance was assumed to be true, that the government's invocation of the state-secrets privilege to remove information from the case was deemed, instead, to give notice under Section 1806(c) of the government's intent to "use" evidence derived from electronic surveillance against plaintiffs. 916 F.3d at 1235. *Fazaga* treated the assertion of the privilege as an

affidavit triggering Section 1806(f)'s procedures. *Id.* And *Fazaga* held that Section 1806(f), without saying so, displaces the dismissal remedy of the state-secrets privilege. *Id.* at 1230-34. *Fazaga* directed that, on remand, "the district court should, using § 1806(f)'s *ex parte* and *in camera* procedures, review any 'materials relating to the surveillance as may be necessary,' 50 U.S.C. § 1806(f), including the evidence over which the Attorney General asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted." *Id.* at 1251.[5]

2. *Fazaga* is fully consistent with the district court's judgment here. *Fazaga* decided the question "whether the procedures established under FISA for adjudicating the *legality* of challenged electronic surveillance replace the common law state secrets privilege with respect to such surveillance to the extent that privilege allows the *categorical* dismissal of causes of action." 916 F.3d at 1226 (emphasis added). The Court there had no occasion to, and did not, hold that plaintiffs can invoke Section 1806(f) procedures to establish threshold issues like Article III

[5] The government has sought rehearing of the panel opinion in *Fazaga*, explaining that Section 1806(f)'s procedures do not apply and that Section 1806(f) does not silently displace the state-secrets privilege. *See* Pet. for Reh'g or Reh'g En Banc, *Fazaga v. FBI*, Nos. 12-56867, 12-56874, & 13-55017 (filed June 14, 2019). If *Fazaga* were to be revised in relevant part, the Court here would have as additional grounds for affirmance that Section 1806(f) is inapplicable even to resolve the merits of plaintiffs' claims (much less standing or aggrieved-person status), and that Section 1806(f), even where it applies, does not displace the state-secrets privilege for purposes of determining the legality of established surveillance (much less for determining whether such surveillance occurred in the first place). *See* ER 27 (district court) ("[A] fair and full adjudication … would require potentially harmful disclosures of national security information that are protected by the state secrets privilege.").

standing or their status as "aggrieved persons." That issue was not presented in *Fazaga* because the plaintiffs' claims there were thrown out on a motion to dismiss, based on the district court's conclusion that resolution of the *merits* of plaintiffs' claims regarding the lawfulness of surveillance, if the case progressed that far, would inevitably endanger state secrets. *Fazaga* simply did not address the standing question presented here; the Court held only that Section 1806(f) procedures can be used to "determine whether surveillance was *lawfully* authorized and conducted," *id.* at 1234 (emphasis added) (quotation mark omitted), if the plaintiffs could establish standing and status as aggrieved persons.

Contrary to plaintiffs' mistaken insistence that *Fazaga* held that "no additional proof of aggrieved-person status beyond well-pleaded allegations is required," Br. 22, *Fazaga* did not resolve an issue it was never presented with, and did not do so in a manner at odds with the text and purpose of Section 1806(f). The *Fazaga* panel instead recognized that, although plaintiffs' bare allegations (accepted as true) had withstood a motion to dismiss, plaintiffs would ultimately need to establish standing and aggrieved-person status on remand by producing evidence: "'The complaint's allegations are sufficient *if proven* to establish that [the plaintiffs] are 'aggrieved persons,'" 916 F.3d at 1216 (emphasis added). And, in its remand instructions to the district court, *Fazaga* noted that "FISA-covered electronic surveillance [may] drop out of consideration" on remand "if, for instance, [the plaintiffs] are unable to substantiate their factual allegations as to the occurrence of the surveillance." *Id.* 1253

& n.52. *Fazaga* is thus consistent with this Court's case law recognizing that aggrieved-person status is a "threshold matter" that a litigant must demonstrate to gain access to Section 1806(f) procedures, not a matter to be decided using Section 1806(f) procedures. *Cavanagh*, 807 F.2d at 789.

And *Fazaga* is consistent with the district court's conclusion that, even if Section 1806(f) procedures were thought to apply to determine these threshold issues, further adjudication of those issues was precluded by the state-secrets privilege. "Critical[]" to *Fazaga*'s analysis of why Section 1806(f)'s procedures should displace the state-secrets privilege for purposes of determining the *legality* of electronic surveillance was the panel's conclusion that such an approach "does not publicly expose the state secrets" submitted *ex parte* and *in camera*. 916 F.3d at 1234. *Fazaga* thus recognized that, to the extent that Section 1806(f) procedures could be thought to displace the dismissal remedy of the state-secrets privilege, those procedures would have that effect only where *ex parte* and *in camera* adjudication would not itself expose state secrets. And while adjudication of the legality of already-disclosed electronic surveillance may or may not risk exposing state secrets, adjudication of the threshold issue of whether there was any such surveillance in the first place would expose what are, here, state secrets. As the district court concluded, and as plaintiffs do not dispute, "even a simple 'yea or nay' as to whether Plaintiffs have standing to proceed on their statutory claims would do grave harm to national security." ER 26. Far from "speak[ing] directly" or clearly to, and requiring, damaging public disclosure of such

information, Section 1806(f) is instead carefully tailored to *avoid* "publicly expos[ing] … state secrets." *Fazaga*, 916 F.3d at 1231, 1234; *see also* S. Rep. No. 95-701, at 65 (emphasizing the importance of giving the government the tools necessary to avoid public disclosures that "would damage the national security"). Consistent with *Fazaga*, then, the district court took all evidence regarding standing into account, *ex parte* and *in camera*, and properly determined that further adjudication of standing would harm national security and present the precise risk that *Fazaga* warned against: "publicly expos[ing] … state secrets." 916 F.3d at 1234.

C. Plaintiffs' Arguments to the Contrary Are Unavailing.

1. In seeking to extend *Fazaga* beyond its holding, plaintiffs do not confront the actual text of Section 1806(f), which provides only that district courts shall use the procedures described in Section 1806(f) to determine the "legality" of electronic surveillance where certain predicates are met. Instead, plaintiffs assert that, where the *ex parte* and *in camera* procedures described in that section may apply to determine the *legality* of surveillance, they also must apply "for *any* purpose, including determining the plaintiff's standing." Br. 18 (emphasis added). Plaintiffs thus insist that, unlike any other civil case, if a plaintiff merely alleges electronic surveillance, claims involving such surveillance "must got forward to a decision on the merits using the procedures of" Section 1806(f), Br. 18—seemingly regardless of plaintiffs' Article III "burden" to establish standing "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). That

atextual proposition is unsupported by any authority and runs counter to the statute's purpose and *Fazaga*'s analysis, as explained above.

Indeed, though Section 1806(f) has existed for over 40 years, plaintiffs have identified no case from any court holding that a plaintiff may rely on privileged evidence to establish standing or status as an "aggrieved person" under FISA. Plaintiffs cite (Br. 23) *In re NSA Telecommunications Records Litigation*, 595 F. Supp. 2d 1077 (N.D. Cal. 2009), which concluded that plaintiffs who plead "aggrieved person" status and withstand a heightened pleading standard on a motion to dismiss thereby "trigger the government's responsibility to affirm or deny" surveillance under Section 1806(f). *Id.* at 1085 (quotation marks omitted). In so concluding, that court "did not conduct an in-depth analysis of the text or indeed even of the legislative history of FISA," which contains no such affirm-or-deny requirement. *Wikimedia*, 335 F. Supp. 3d at 785. And, in any event, the same district court also concluded, consistent with the district court here, that the plaintiffs there "must first establish 'aggrieved person' status without the use of" information subject to the state-secrets privilege, even though the court also concluded that such privileged evidence "might well" be considered later if plaintiffs adequately established their "aggrieved person" status and if Section 1806(f) procedures were triggered. *In re NSA Telecomms. Records Litig.*, 564 F. Supp. 2d 1109, 1134 (N.D. Cal. 2008).

2. Plaintiffs mistakenly insist that the district court's ruling upholding the state-secrets privilege contradicts the court's earlier rulings concluding (like *Fazaga*) that

Section 1806(f), where it applies, displaces the state-secrets privilege in certain applications. *See* Br. 19. There is no such contradiction. The district court, in the same order concluding that Section 1806(f) displaces the privilege, expressly warned that even if Section 1806(f) "provides the mechanism for review," plaintiffs "shall be tasked with the burden to establish standing to sue without resulting in impermissible damage to ongoing national security efforts." ER 79 (citing *Clapper*, 568 U.S. at 412 n.4); *see also* ER 70 (Section 1806(f) "preempts or displaces the state secrets privilege, but only in cases within the reach of its provisions.").

Plaintiffs are similarly mistaken in asserting that the district court "noted but did not adopt" the argument that the court "could not proceed under section 1806(f) unless plaintiffs first" established standing and aggrieved-person status "using public evidence." Br. 21. To the contrary, the district court held that "[p]laintiffs must, using *publicly available facts*, adduce admissible evidence that the contents of their communications or the metadata regarding those communications were subject to the intelligence-collection activities they challenge in this case." ER 12 (emphasis added).

3. Plaintiffs query (Br. 23) why Congress would require a person to establish his or her standing and status as an "aggrieved person" subject to surveillance as a precondition to the district court determining the lawfulness of the surveillance. In addition to the obvious mischief that the Supreme Court recognized when rejecting an *in camera* procedure in *Clapper*, 568 U.S. at 412 n.4, plaintiffs continue to ignore how litigants may learn of their aggrieved-person status and thus be in a position to

potentially have the legality of the surveillance determined using Section 1806(f). The government must give notice when it intends to use evidence derived from electronic surveillance against an aggrieved person in a proceeding. 50 U.S.C. § 1806(c); *United States v. Ott*, 827 F.2d 473, 475 (9th Cir. 1987) (defendant in a court-martial provided with notice). And plaintiffs can try to establish standing using their own evidence or officially disclosed information, so long as standing can be litigated without unacceptable risk to national security. *See Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007) (a claim might proceed "if the plaintiffs can prove the essential facts of their claims without resort to material touching upon military secrets" (quotation marks omitted)); *Jeppesen Dataplan*, 614 F.3d at 1082-83.

For understandable reasons, however, Congress did not create a system whereby any person can simply file a complaint that meets basic pleading requirements in which plausibly alleged facts must be taken as true, and thereby, as a matter of course, force the government (or a court, through its ruling) to reveal whether the person's communications have been subject to surveillance, irrespective of the harm to national security that may arise from such a disclosure. To the contrary, Congress designed Section 1806(f) to give the government the tools to protect against such damaging public disclosures. *See* S. Rep. No. 95-701, at 65. As a result, some plaintiffs (as here) may ultimately not be able to establish standing. But, as this Court has recognized, "[w]hile dismissal of an action based on the state secrets privilege is harsh, the results are harsh in either direction," because publicly disclosing

state secrets would damage the national security, "and the state secrets doctrine finds the greater public good—ultimately the less harsh remedy—to be dismissal." *Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998) (quotation marks omitted).

4. Finally, plaintiffs appear to offer an alternative rationale, suggesting that a provision of the Stored Communications Act, 18 U.S.C. § 2712(b)(4), provides for *in camera* and *ex parte* determination of standing even if Section 1806(f) does not. *See* Br. 17-18, 24. The provision they cite does no such thing. Plaintiffs invoke a cause of action that authorizes "[a]ny person who is aggrieved by any willful violation of" certain provisions of FISA, the Wiretap Act, and the Stored Communications Act, to "commence an action … against the United States to recover money damages." 18 U.S.C. § 2712(a). A subsection of the same provision refers to FISA procedures: "[n]otwithstanding any other provision of law, the procedures set forth in" three provisions of FISA—Section 1806(f), regarding electronic surveillance, and two parallel provisions regarding physical searches and pen registers, *see* 50 U.S.C. §§ 1825(g), 1845(f)—"shall be the exclusive means by which materials governed by those sections may be reviewed." 18 U.S.C. § 2712(b)(4).

Section 2712(b)(4) thus prohibits a plaintiff from bypassing the government-protective FISA procedures, where those procedures are applicable, simply by invoking the cause of action in Section 2712(a). In doing so, Section 2712(b)(4) takes Section 1806(f)'s procedures as it finds them: it makes those procedures "the exclusive means by which materials governed by [Section 1806(f)] may be reviewed."

18 U.S.C. § 2712(b)(4). The cross-reference to Section 1806(f) does not work a silent revolution in how the referenced procedures operate. It does not re-write Section 1806(f) to remove the threshold "aggrieved-person" requirement. To the contrary, consistent with that requirement in Section 1806(f), the cause of action in Section 2712(a) similarly requires that the person be "aggrieved." And the "materials governed by" Section 1806(f), to which Section 2712(b)(4) refers, are defined in Section 1806(f) as "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," 50 U.S.C. § 1806(f)—not materials as may be necessary to determine whether "the surveillance" occurred in the first place, or whether plaintiffs are "aggrieved persons."

II. Plaintiffs Cannot Establish Standing.

The district court thus correctly denied plaintiffs' motion to determine standing on the basis of privileged information using the *ex parte* and *in camera* procedures described in Section 1806(f). And if this Court were to agree, it would not need to resolve the myriad evidentiary issues discussed in the rest of Part II.

Plaintiffs' only arguments on appeal regarding the state-secrets privilege are their erroneous assertions that (1) Section 1806(f)'s procedures apply to determine aggrieved-person status (rather than requiring that showing as precondition), and (2) Section 1806(f)'s procedures displace the state-secrets privilege in that application. Plaintiffs do not separately argue that, if the privilege is applicable, the district court

erred in upholding it here, or in concluding that (3) it required dismissal because litigation about whether plaintiffs were subject to electronic surveillance would pose an unacceptable risk of disclosing state secrets. *See Jeppesen Dataplan*, 614 F.3d at 1082-83. "[A]ny determinative finding on the issue of whether" plaintiffs were subject to alleged surveillance "may result in potentially devastating national security consequences." ER 21 ("Any attempt to prove the specific facts of the programs at issue, or to defend against the Plaintiffs' analysis … would risk disclosure of … operational details," which "could be expected to cause exceptionally grave damage to national security."); *see also* NSA Dir. Rogers Decl. ¶¶ 324-84 (explaining the risks).

Thus, regardless of the evidentiary issues discussed below, if plaintiffs are wrong as to (1), and Section 1806(f) requires a threshold showing of aggrieved-person status, plaintiffs have no means of making that showing consistent with the state-secrets privilege because, as they do not dispute, (3) litigating that issue would expose state secrets. And even if (1) Section 1806(f) procedures could be thought to apply to make the predicate factual determination whether plaintiffs were subject to electronic surveillance, plaintiffs still make no argument that the district court erred in concluding that (3) such a determination could not be made, even using Section 1806(f) procedures, without exposing state secrets. Thus, the evidentiary issues below are irrelevant if plaintiffs are wrong about either or both of propositions (1) and (2).

In any event, as the district court correctly held, plaintiffs identify no non-privileged evidence showing they were subject to the alleged intelligence-gathering

activities they seek to challenge. As "[t]he party invoking federal jurisdiction," plaintiffs carry the "burden" of establishing standing "with the manner and degree of evidence required at the successive stages of the litigation." *Lujan*, 504 U.S. at 561. This Court held in 2011 that the allegations in plaintiffs' complaint, "accept[ed] as true" in that procedural posture, were sufficient to support standing on the pleadings. *Jewel v. NSA*, 673 F.3d 902, 910-11 (9th Cir. 2011). But this Court warned that, at summary judgment, plaintiffs might "[u]ltimately" be "unable to produce any evidence that any of their own communications have ever been intercepted," and that such "failure of proof" at that procedural stage may therefore "doom[] [their] standing." *Id.* at 911 (quotation marks omitted). And, as this Court contemplated, plaintiffs ultimately were unable to introduce competent evidence showing that their own communications (or metadata about their communications) have, in fact, been subject to the intelligence-gathering programs that plaintiffs seek to challenge. The district court thus properly granted summary judgment for lack of standing.

A. Bulk Telephony Metadata

The government used to (but not longer does) collect in bulk certain call-detail records, or metadata about telephone calls, such as dates, times, durations, and originating and receiving numbers. SER 41-42, 54-55 (Rogers Decl.). The government used the collected information to help detect communications between suspected terrorists and other operatives. SER 55. Where analysts had a reasonable articulable suspicion to believe that a known phone number was associated with a

terrorist, analysts could query the bulk metadata that had been collected to determine what other phone numbers within the collected metadata had been in direct contact with the initial number (and those in direct contact with the contacts, out to two or three degrees of removal from the first number). SER 55-56.

In order to support their Article III standing to challenge the since-discontinued bulk collection of telephony metadata, plaintiffs must introduce evidence showing that metadata relating to their calls was collected. At summary judgment, it is not enough for plaintiffs to put forward only "some evidence" or a "mere … scintilla" supporting standing. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 251-52 (1986). Instead, it is plaintiffs' obligation to introduce enough evidence supporting "specific facts" that could warrant "a verdict in [plaintiffs'] favor" on the issue of standing "based on that evidence." *T.W. Elec. Serv., Inc. v. Pacific Elec. Contractors Ass'n*, 809 F.2d 626, 631-32 (9th Cir. 1987).

1. Plaintiffs here submitted no evidence that could establish either that the government collected *all* metadata of all telephone calls in the United States (therefore by definition including metadata about their own calls), or that the government, collecting less than all metadata, actually sought and collected metadata about plaintiffs' particular calls. *See Schuchardt v. President of the U.S.*, 839 F.3d 336, 349, 354 n.13 (3d Cir. 2016) (noting these two potential paths to establish standing to challenge alleged untargeted surveillance). Evidence that plaintiffs used phones while the program was operating is insufficient to establish standing because, while the bulk

telephony metadata program was "broad in scope and involved the collection and aggregation of a large volume of data from multiple telecommunications service providers," the government has made clear in sworn testimony that "it never captured information on all (or virtually all) calls made and/or received in the U.S." SER 55 (Rogers Decl.). Plaintiffs do not dispute this evidence.

Nor do plaintiffs point to any non-privileged, admissible evidence showing that metadata about their communications in particular was collected. The government has officially declassified only one order that compelled a single telecommunications service provider—Verizon Business Network Services—to produce telephony metadata in bulk for a single 90-day period in 2013. SER 56-57 (Rogers Decl.). Plaintiffs offer no evidence that they subscribed to that particular service provider, much less during the relevant time period. Besides confirming collection from that one provider for that single, brief period, the government has consistently refrained from either confirming or denying whether other providers participated in NSA bulk collection of telephony metadata. *Id.* The identities of participating providers have not been officially disclosed, and remain properly classified state secrets. *Id.*; SER 9, 14-15 (Gordon Decl.). It is thus unsurprising that plaintiffs identify no admissible evidence that would allow a trier of fact to conclude that metadata about their telephone communications was collected.

2. Plaintiffs chiefly rely (Br. 27, 31-32) on the government's public characterizations of the size of the bulk telephony metadata program, drawn from

declassified court opinions and a report of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent Executive agency that "review[s] actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties." 42 U.S.C. § 2000ee(c)(1). But those characterizations of the program do no more than repeat what the government has already said: the program involved the collection of a large volume of data. That says nothing about whether metadata about *plaintiffs'* numbers was collected.

Plaintiffs speculate that the "size and method" of the bulk phone records program necessarily means that "it could not have operated without participation of" their phone service providers, AT&T and Verizon. Br. 30.[6] That argument rests on numerous flaws. First, plaintiffs wrongly assert that the NSA's searches of collected bulk metadata "in 2012 alone" actually "yielded the phone records of 120 million persons." Br. 31. In fact, the report on which plaintiffs rely merely calculated, by way of illustration, how many phone numbers hypothetically "would" be examined in a search of 300 initial numbers of interest, assuming that each direct contact, out to the

[6] Similarly unavailing is plaintiffs' reliance on two public reports from AT&T and Verizon stating that each received in recent years between "0" and "499" demands for non-content information under FISA. ER 911, 928. Those reports do not establish that either company received more than zero requests and, in any event, do not specifically address bulk telephony metadata collection. *See* ER 927 (Verizon report) (noting that reported ranges do not include "any orders we may have received related to the bulk collection of non-content information").

third "hop," had 75 unique direct contacts, and assuming that metadata for each such contact had been collected. ER 184-85. That illustration was not based on actual data about the size or scope of the program. And the mathematical result that 75 cubed, multiplied by 300, yields a number close to 120 million says nothing about whether the government was, in fact, collecting metadata about that or any other set of phone numbers.[7]

Plaintiffs further speculate that it would not be "mathematically possible" for the government to have records about 120 million phone numbers that could be returned by searches, without collecting records from their phone services providers, AT&T and Verizon. Br. 32. But plaintiffs present no evidence that the program was actually collecting that many records. Plaintiffs also offer no evidence or explanation to support their bare assertion that metadata about 120 million numbers (even if that number were relevant) could not be collected from other providers.[8]

Plaintiffs try to invoke the alleged size of their respective telephone providers and insist that, even if they cannot individually show that metadata was collected from any particular providers, they nonetheless have collective standing because, they

[7] Small variations in assumptions, when raised to the third power, can lead to large differences in results, as 50 cubed times 300 is less than 38 million, while 100 cubed times 300 is 300 million.

[8] *Compare* Br. 31 n.9 (requesting judicial notice of what plaintiffs say were 163 million AT&T customer phone lines and 128 million Verizon customer phone lines in 2018), *with* Federal Communications Commission, *Numbering Resource Utilization in the United States* 4 (Apr. 2013), https://go.usa.gov/xpmaq (reporting that "about 677 million telephone numbers were assigned to end users" in the United States in 2010).

assume, the bulk metadata program would not have excluded *all* of those providers. *See* Br. 31-32 ("A program that excluded AT&T and Verizon certainly could not perform three-hop searches yielding the phone records of 120 million persons."). But "[s]tanding is not dispensed in gross." *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 353 (2006). Nor is it dispensed "probabilistic[ally]" to aggregated groups. *Summers v. Earth Island Inst.*, 555 U.S. 488, 499 (2009). Each plaintiff must make out his or her own standing with respect to each form of relief sought, on the basis of each plaintiff's own injury.

Nor are plaintiffs' unfounded assumptions about the government's surveillance goals, resources, constraints, and priorities sufficient to support standing. Plaintiffs insist that the government should be assumed to have collected bulk metadata from their phone providers because, in their view, doing so would make searches of collected metadata more "reliabl[e]" and avoid missed connections. Br. 31. But the Supreme Court foreclosed that kind of conjecture as a basis to support standing on summary judgment in *Clapper v. Amnesty International*. The Supreme Court's majority opinion rejected reliance on what the dissent termed the "commonsense inference[]" that there was a "high probability" of injury. 568 U.S. at 427-31 (Breyer, J., dissenting) (referring to plaintiffs' allegations that they communicated with non-U.S. persons abroad about foreign-intelligence information, that the government assertedly had a "strong motive" and "capacity" to collect those communications, and that the government had previously collected, under another surveillance authority, tens of

thousands of communications involving a person with whom one plaintiff communicated regularly). Because plaintiffs there had "no actual knowledge" of the government's surveillance practices and "[i]nstead … merely speculate[d] and ma[d]e assumptions about whether their communications … will be acquired," their "allegations [were] necessarily conjectural" and did not establish standing. *Id.* at 411-12 (majority).

The D.C. Circuit has applied *Clapper* to reject standing arguments in a challenge to the same bulk telephony metadata program at issue here. *See Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam). A majority of the judges there explained that the *Klayman* plaintiffs' "contention that the government is collecting data from Verizon Wireless … depends entirely on an inference from the existence of the bulk collection program itself," and the plaintiffs' assumption that "[s]uch a program would be ineffective … unless the government were collecting metadata from every large carrier." *Id.* at 565 (Williams, J., concurring); *see also id.* at 569-70 (Sentelle, J., dissenting in part and agreeing with Judge Williams's standing analysis). But this "case for standing is similar to that rejected in *Clapper,*" as the plaintiffs' "assertion that NSA's collection must be comprehensive in order for the program to be most effective is no stronger than the *Clapper* plaintiffs'" similar assertions. *Id.* at 567 (Williams, J.).

As in *Clapper* and *Klayman*, plaintiffs here have no actual knowledge of the government's practices in collecting bulk metadata about phone calls. And their

assumptions about the government's motives and capacity are, as the district court correctly held, "no stronger than the *Clapper* plaintiffs' assertions regarding the government's motive and capacity to target their communications." ER 15 (quoting *Klayman*, 800 F.3d at 567 (Williams, J.)). Just as the Supreme Court "necessarily found that [the *Clapper*] plaintiffs' inferences were inadequate even to preserve the question of standing as a 'genuine issue,'" *Klayman*, 800 F.3d at 568 (Williams, J.), the same is true here. *Cf. Al-Haramain*, 507 F.3d at 1203 (rejecting "judicial intuition about" whether "the very existence of" a surveillance program "suggest[s] that the government is in fact intercepting [a plaintiff's] communications").

3. Plaintiffs also seek to rely on two unauthenticated documents, something they call the "NSA letter," Br. 28, and another document they call the "NSA Draft OIG report," Br. 29, 35-36. But neither document is or can be "presented in a form that would be admissible in evidence," Fed. R. Civ. P. 56(c)(2), because plaintiffs cannot "produce evidence sufficient to support a finding that the item is what the proponent claims it is," Fed. R. Evid. 901(a); *see Orr v. Bank of Am., NT & SA*, 285 F.3d 764, 773 (9th Cir. 2002) ("Authentication is a 'condition precedent to admissibility.'") The district court thus did not abuse its discretion in excluding those documents from consideration at summary judgment.

a. Plaintiffs contend that, in the so-called "NSA letter," the "government disclosed" their phone providers' "participation in the phone records program." Br. 27. But, as the district court correctly held, the identity of telecommunications

providers who may or may not have participated in the bulk program remains a highly classified state secret, the authenticity of the letter itself is thus likewise a state secret "the disclosure of which could reasonably be expected to cause grave harm to national security," and the document could thus not be relied on as admissible evidence to support standing. ER 18-19.

The government has publicly released a "primary order" from the FISC that authorized the bulk collection of telephony metadata under FISA but redacted the identities of service providers that could later be compelled to provide bulk metadata. ER 849. Plaintiffs assert that the "NSA Letter," which purports to have been sent from the NSA to the FISC, refers to the primary order as having "requir[ed] the Production" of bulk telephony metadata "from AT&T" and "Verizon Wireless." ER 896.

That document has not been and cannot be authenticated, and plaintiffs accordingly cannot rely on it to establish that any particular telephone providers participated in bulk metadata collection. In an unsuccessful attempt to render the document admissible, plaintiffs submitted an affidavit from a lawyer for a newspaper stating that the letter had been "inadvertently produced" to him under the Freedom of Information Act, that the government had "asked for its return," and that the newspaper had then published an article based on the letter. ER 148.

But plaintiffs' reliance on that affidavit is foreclosed by *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190 (9th Cir. 2007), where the government

"inadvertently" disclosed a certain Sealed Document, marked as Top Secret, which the plaintiffs and their attorneys read and retained, and which they alleged supported their claims that their communications had been subject to the surveillance they sought to challenge. *Id.* at 1193, 1194-95. This Court held that, despite the inadvertent disclosure, "[t]he Sealed Document, its contents, and any individuals' memories of its contents, even well-reasoned speculation as to its contents, are completely barred from further disclosure in this litigation by the common law state secrets privilege." *Id.* at 1204-05. The same results follow here, and for the same reasons.

Plaintiffs seek to distinguish *Al-Haramain* because the document at issue here purportedly was inadvertently disclosed to a newspaper, which published an article about it, while the Sealed Document in *Al-Haramain* had been inadvertently disclosed to the plaintiffs themselves, disseminated to and read by various members of the plaintiff group, retained by members of the group for litigation, and shared with a reporter from the Washington Post who was conducting research for a book. Br. 33-34; *Al-Haramain*, 507 F.3d at 1195. But there is no reasoned basis to conclude the privilege over the contents of the Sealed Document in *Al-Haramain* would have evaporated if, as here, the putative recipient had uploaded the document to the internet or published a news story about it. Indeed, such a rule would create truly perverse incentives that would further risk national security any time there may be an inadvertent disclosure.

Plaintiffs misunderstand *Al-Haramain* to permit a court to second-guess whether the contents and authenticity of a document "remain[] secret" and privileged. Br. 34. But *Al-Haramain* merely discussed with approval the district court's determination there that the Sealed Document, and its contents, "remain[] secret" specifically "because *the government has not officially confirmed or denied* whether plaintiffs were subject to surveillance, even if plaintiffs know they were." 507 F.3d at 1202 (emphasis added) (quotation marks omitted). The same is true here. There is no basis for this Court or the district court to assume—contrary to the valid assertion of the state-secrets privilege—the authenticity of the document here, merely because plaintiffs claim to know its provenance, when its authenticity (or lack thereof), and the truth or falsity of its contents, is a state secret.

This Court's recent opinion in *Husayn v. Mitchell*, 938 F.3d 1123 (9th Cir. 2019), is not to the contrary. The panel there held that "in order to be a 'state secret,' a fact must first be a 'secret,'" *id.* at 1133, concluding that the state-secrets privilege did not apply to certain matters acknowledged by the European Court of Human Rights and Polish government officials, *id.* at 1134. Here, no one has officially acknowledged the information over which the government invokes the privilege. And the *Husayn* panel upheld the privilege with respect to details that went beyond the purported acknowledgement by foreign officials, including "documents, memoranda, and correspondence about the identities and roles of foreign individuals involved with the detention facility, operational details about the facility, and any contracts made with

Polish government officials or private persons residing in Poland," as these materials "might implicate the CIA's intelligence gathering efforts." *Id.* at 1134. Similarly, the government here has officially acknowledged the existence of the bulk telephony metadata program; all it seeks to protect, consistent with *Husayn*, are state secrets regarding, as relevant here, the details concerning the identity of any telecommunications companies that may or may not have participated in the program, and the authenticity (or lack thereof) of the document at issue here. *See Jeppesen Dataplan*, 614 F.3d at 1090 ("[P]artial disclosure of the existence and even some aspects of the extraordinary rendition program does not preclude other details from remaining state secrets if *their* disclosure would risk grave harm to national security.").

b. Similarly, the document that plaintiffs call the "NSA Draft OIG report," which they obtained from a website, is inadmissible because it cannot be authenticated. That document purports to be a draft report from the NSA's Office of the Inspector General. ER 93. And it purports to identify "COMPANY A" and "COMPANY B" (without further elaboration) as having participated in the bulk telephony metadata program under the President's Surveillance Program. ER 128. In an attempt to render this document admissible, plaintiffs filed an affidavit executed by Edward Snowden saying that he "became familiar with" and "read" this supposed draft report while working at an NSA facility. ER 88. But like the so-called "NSA Letter," the authentication (and hence admissibility) of this document is precluded by the state-secrets privilege. ER 18-19; *Al-Haramain*, 507 F.3d at 1205.

In any event, Snowden cannot authenticate the document through personal knowledge, Fed. R. Evid. 901(b)(1), because he does not even purport to be prepared to testify that he "wrote it, signed it, used it, or saw others do so." *Orr*, 285 F.3d at 774 n.8.[9] Nor can plaintiffs authenticate the document by contending that its "appearance, contents, substance, internal patterns, or other distinctive characteristics" show it to be what plaintiffs claim it is, Fed. R. Evid. 901(b)(4), as plaintiffs have identified no basis by which anyone could determine the typical or distinctive features of a Top Secret working draft of an internal NSA report. *See United States v. One 56-Foot Motor Yacht Named Tahuna*, 702 F.2d 1276, 1284 (9th Cir. 1983) (authenticating a diary under Rule 901(b)(4) by comparing its contents with independent evidence, such as known aliases and physical addresses).

Nor can the document be authenticated on the ground that it is "a purported public record or statement [that] is from the office where items of this kind are kept." Fed. R. Evid. 901(b)(7)(B). Plaintiffs do not explain how a document marked "Top Secret" is a "public" record. And Snowden does not assert that he was the

[9] Plaintiffs are also unable to present Snowden's proffered testimony in admissible form. Fed. R. Civ. P. 56(c)(2). The declaration is hearsay to which no exception applies. *See* Fed. R. Evid. 801(c), 804(b). And there is no other form in which Snowden, who has fled the country and resides in Russia, can present admissible testimony at trial. The district court was presented with these arguments, *see* Gov't Defs.' Sur-Reply 2-3, ECF 439, and correctly concluded that Snowden's testimony was inadmissible, "either by way of his current declaration or in the future through live testimony." ER 19. Plaintiffs' opening brief notes that conclusion, Br. 35-36, but presents no contrary arguments.

"custodian" of the document or the file where it was purportedly kept. *See United States v. Lopez*, 762 F.3d 852, 863 (9th Cir. 2014) (noting that this Court has upheld authentication of public records where the custodian testified).

B. Bulk Internet Metadata

Plaintiffs similarly have no standing to challenge the discontinued programs that used to, but no longer do, collect certain bulk metadata about internet communications, such as the "to" and "from" lines of emails. SER 58 (Rogers Decl.).

As described by declassified court orders authorizing the government to collect certain bulk internet metadata, analysts used the collected metadata to "uncover new terrorists." ER 667. By searching metadata using identifiers, like email addresses, reasonably suspected of being associated with a terrorist, analysts could identify other email addresses that had been in contact with the initial address (and those who were in contact with those contacts, *i.e.*, the second "hop"). ER 678.

The government was initially authorized to collect bulk internet metadata at a discrete set of unidentified facilities, ER 672, and with regard to a discrete set of unidentified categories of metadata, ER 627. The scope of collection that was *authorized*—including the "volume of metadata" and "range of facilities"—grew over time, but court orders recognized that "NSA does not expect to *implement* the full scope of the requested authorization." ER 663-64 (emphasis added). Ultimately, "[u]pon concluding that the program's value was limited," the government terminated the program. ER 195 (PCLOB report).

The government has acknowledged that the court-authorized program, while it existed, "operated on a large scale." SER 58 (Rogers Decl.). But the government has not publicly "specif[ied] its scope or the identities of any participating providers," *id.*, which remain highly classified state secrets, SER 9, 14-15 (Gordon Decl.). It is thus unsurprising that, as with the programs that collected bulk *telephony* metadata, plaintiffs identify no admissible evidence that would allow a trier of fact to conclude that metadata about their *internet* communications was collected—*i.e.*, that they are "among the injured." *Lujan*, 504 U.S. at 563 (quotation marks omitted). The district court thus did not err in concluding that plaintiffs' unsupported assumptions about the size and scope of the internet metadata program did not support standing. ER 15.

Plaintiffs point (Br. 57) to the so-called "Draft NSA OIG report," which states only that the President's Surveillance Program collected unspecified internet metadata from certain "data links owned or operated by COMPANIES A, B, and C." ER 129. But, as discussed above, *see supra* pp. 47-49, the district court did not abuse its discretion in holding, ER 19, that the authenticity of that proffered document has not been shown and is protected in any event by the state-secrets privilege (and therefore cannot be used to support plaintiffs' standing on summary judgment). *See Al-Haramain*, 507 F.3d at 1205.

Moreover, the so-called draft report, even on its own terms, does not claim that all or even most metadata about communications of subscribers to services provided by Companies A, B, and C were collected; it does not claim that collection involved all

or most of those companies' "data links"; and it does not claim that collection involved all or most of the metadata about communications passing through any targeted "data links." To the contrary, the proffered document asserts that "NSA took great care to ensure that metadata was produced against foreign, not domestic communications" and "vetted" the "data links" accordingly. ER 129. Plaintiffs speculate that what they say is happening at an AT&T facility in San Francisco (discussed below) "*could* also be used to collect Internet metadata." Br. 58 (emphasis added). But they do not point to any actual evidence. Plaintiffs instead rely entirely on what they think "the classified evidence should show," *id.*, but such evidence, whatever it shows, is privileged.

Plaintiffs' experts do not make up for these evidentiary shortfalls. As a preliminary matter, plaintiffs have forfeited reliance on their experts for their internet metadata claims by "inadequately brief[ing]" the issue below and on appeal. *Brownfield v. City of Yakima*, 612 F.3d 1140, 1149 n.4 (9th Cir. 2010) ("We will not manufacture arguments for an appellant, and a bare assertion does not preserve a claim, particularly when, as here, a host of other issues are presented for review."). Plaintiffs' brief asserts that "Internet communications routing" is "essentially random" and that this somehow means that "wherever" the government may have collected internet metadata—that is, regardless of any actual details about the type or number of facilities used for collection, what is collected, and how—the government must have collected metadata from "at least one of each plaintiffs' communications." Br. 57.

This argument is no stronger in this context than it was when discussing telephony metadata: plaintiffs cannot rely on an assumption about the scale of the program to assert that metadata about their communications, collectively, must have been collected.

And plaintiffs' sweeping conclusion is unsupported by their unexplained string cite. Br. 57. Nothing in the cited expert declarations says that internet communication routing is inherently "random," or that the location and method of metadata collection would be irrelevant to whether plaintiffs were subject to surveillance. To the contrary, two of the declarations offer reasons why the experts think it likely that some of plaintiffs' internet communications would have been routed through a particular AT&T facility in San Francisco. ER 973, 989. But nothing in those declarations, or any other evidence, supports the bare speculation in plaintiffs' brief (Br. 58) that internet metadata collection, and collection of metadata about their communications in particular, "could" have occurred at that facility. And, in any event, those declarations would be inadequate to support plaintiffs' standing to challenge bulk internet metadata collection for the same reason, as explained below, that they do not support plaintiffs' standing to challenge targeted content collection alleged to be occurring at that facility.

A third expert avers that a "surveillance program directed solely at foreign communications" "likely"—he doesn't say how likely— "would result in the collection of even" some unspecified "purely domestic communications belonging to

American users of cloud-based applications." ER 998. But the issue here is whether plaintiffs *themselves* were "among the injured," *Lujan*, 504 U.S. at 563 (quotation marks omitted), and the district court did not abuse its discretion in concluding, ER 17, that the expert does not adequately address that issue.

C. Targeted Collection of Certain Internet Content

1. Under the President's Surveillance Program, the government engaged in targeted—not bulk—collection of the content of certain communications reasonably believed to involve agents of al-Qaida or other terrorist organizations. SER 41-42, 59, 66 (Rogers Decl.). Later, that program was terminated and the government began court-authorized targeted content collection, first under transitional statutory authority, and then under FISA Section 702. *See* ER 413-17 (PCLOB report). Section 702 provides that, with targeting and minimization procedures approved by the FISC, the government may "target[] . . . persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. §§ 1881a(a), 1881a(j). Among other significant limitations on this authority, the government may not target "any person known at the time of acquisition to be located in the United States" or "a United States person reasonably believed to be located outside the United States." *Id.* § 1881a(b)(1), (3). And collection "shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States." *Id.* § 1881a(b)(6).

Collection under Section 702 occurs with regard to a specific, tasked electronic communication selector, such as an email address, using a directive issued to an appropriate electronic communications service provider compelling the provider's assistance in the acquisition of targeted communications involving the selector. 50 U.S.C. § 1881a(i)(1). If, for example, the government identifies an email address used by a member of a foreign terrorist organization located abroad, that selector could be chosen for targeted content collection under Section 702. ER 429-30, 438-44 (PCLOB report). Plaintiffs seek to challenge "upstream" collection of a tasked selector (such as an email address), so called because it "occurs 'upstream' in the flow of communications between communication service providers" with the "compelled assistance … of the providers that control the telecommunications backbone over which communications transit." ER 432.

Plaintiffs do not dispute that the internet content collection they challenge is targeted, not bulk, collection. They do not argue that their electronic communications selectors have been targeted for collection, that the government has targeted anyone with whom they communicate, or that any of their communications have ever actually been ingested into government databases. Instead, plaintiffs assert that their speculation about how targeted upstream collection works supports their belief that their internet communications must at some point have passed through what they think are government surveillance devices. But the record evidence does not support their claim to standing.

The government has explained in general terms how upstream collection works: Tasked selectors (such as email addresses) "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.'" ER 433-34 (PCLOB report). "Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector." ER 434. "Unless transactions pass both these screens, they are not ingested into government databases." *Id.* Though the government has disclosed certain high-level descriptions of upstream collection, "the specific sources and methods used under the [President's Surveillance Program], and Section 702, to intercept the content of communications" remain highly classified state secrets. SER 9, 13 (Gordon Decl.).

Plaintiffs think they can fill in those details with their own speculation. But that is no basis for standing. Plaintiffs claim that upstream collection occurs by means of the NSA "cop[ying]" "[a]ll of the communications" on monitored fiber-optic cables using optical splitters, redirecting the copied stream of communications so that the NSA may filter out domestic communications and scan for tasked selectors. Br. 65-67. Plaintiffs argue that copying and redirecting communications, *alone*, injures the senders and receivers of those communications within the meaning of Article III's standing requirement, even if the original communication is not impeded and even if

the supposedly copied, scanned, and discarded communications are never seen or used by anyone. Br. 42-43 n.13.

The district court had no occasion to resolve the question whether such alleged copying could give rise to a cognizable injury because the court concluded, at the threshold, that plaintiffs failed to introduce admissible evidence showing that their *own* communications were subject to any such alleged copying "controlled by or at the direction of the Defendants." ER 15. That conclusion is correct and should be upheld. Plaintiffs submitted no admissible evidence that AT&T has helped facilitate the NSA's acquisition of internet content under the President's Surveillance Program or Section 702,[10] much less any evidence regarding where or how such alleged collection occurs or evidence that this collection included plaintiffs' communications. Indeed, plaintiffs identify no evidence supporting their bare allegation that upstream collection even involves a "copying" step at all.

Plaintiffs attempt to show that they are among those allegedly "injured" by raising factual assertions about what was happening in 2003 in a particular AT&T facility located on Folsom Street in San Francisco. Br. 39-41. Plaintiffs contend that

[10] Plaintiffs mistakenly rely (Br. 39, 44) on a report saying that AT&T has received orders requiring the production of the content of communications under FISA. ER 911. That report does not say what provision of FISA authorized those orders, or even whether those orders related to NSA surveillance. Plaintiffs also mistakenly rely (Br. 38, 44) on what they call the "NSA Draft OIG report," which refers to "Company A" as supposedly having participated in internet content collection. ER 128. As discussed above, *see supra* pp. 47-49, the authenticity (or lack thereof) of that document is privileged, and the document cannot be authenticated.

(1) at least one of each of their communications has gone through fiber-optic cables at that facility; (2) an optical splitter copies and diverts the entire stream of communications passing over those cables at that facility; (3) the copied information is sent to the so-called SG3 room at the facility; and (4) in the SG3 room, the NSA filters and scans for tasked selectors.

But even if plaintiffs could show that their communications transited fiber-optic cables in that facility, that those communications were copied and diverted by an optical splitter, and that they were sent to the SG3 room (*i.e.*, propositions 1, 2, and 3), plaintiffs have still failed to introduce admissible evidence as to the NSA's supposed involvement in copying and diverting the communications to the SG3 room, or any evidence to support their speculation about what happens in the SG3 room, much less evidence supporting the allegations that the NSA uses that room to filter and scan communications to facilitate upstream collection. And because plaintiffs introduced no admissible evidence to establish that their claimed injury is fairly traceable to defendants, the district court correctly granted summary judgment. *See Clapper*, 568 U.S. at 409.

2. The linchpin of plaintiffs' allegations that the NSA has any control or direction over whatever happens at the San Francisco facility is a 13-year-old declaration from a former technician, Mark Klein, who worked at the AT&T facility briefly before retiring in 2004. ER 1206-15. Klein states that in February 2003 optical splitters were installed on certain fiber-optic cables carrying internet communications

to and from various other telecommunications networks and that these splitters sent a copy of the communications passing through those cables into a newly constructed "SG3" room. ER 1214. By Klein's own account, he had "extremely limited access" to the SG3 room—he entered it only once—and he does not claim to have personally observed any relevant contents of the room or activities occurring in the room. ER 1212. As the district court correctly noted, "Klein can [thus] only speculate about what data were actually processed and by whom in the secure room and how and for what purpose, as he was never involved in its operation." ER 16.

a. Whatever was happening in the room, Klein thinks (but cannot prove) the NSA was somehow involved: An unnamed supervisor "told [Klein]" to expect an "NSA agent" to visit some other AT&T facility "to interview" another person "for a special job," which the supervisor "later confirmed to [Klein] … was at the Folsom Street Facility" in San Francisco. ER 1211.[11] But the supervisor's out-of-court statements that an "NSA agent" would be interviewing people for a job in the SG3 room is hearsay (with no demonstrated basis in the supervisor's personal knowledge) and cannot be admitted as evidence for the truth of the matter asserted, Fed. R. Evid. 801, 802, and the district court did not abuse its discretion in so holding, ER 17.

[11] Klein also says he "received an email" about a pending visit that "explicitly mentioned the NSA." ER 1211. And, similar to the first alleged interview, Klein says that a supervisor "told [him] that another NSA agent would again visit" some other AT&T facility to learn about another person's "suitability to perform the special job" the first interviewee "had been doing." ER 1212. And "[b]y January 2004," the new person "had taken over the special job." *Id.*

Plaintiffs attempt to avoid the hearsay rule by noting that an employee can testify about his or her own observations and experiences. Br. 49-53. But Klein does not say he had any observations or experiences that gave him personal knowledge that an "NSA agent" interviewed someone for a job at the SG3 room. Klein does not say that he observed or participated in that event. And Klein's assertions of *NSA* involvement all trace back to hearsay: Klein says he thinks that the interviewer was an "NSA agent" because someone told him so; Klein asserts no other basis for that belief.[12]

Plaintiffs also contend (Br. 52) that the supervisor's statements are not hearsay because they were allegedly "made by [the NSA's] agent … on a matter within the scope of that relationship." Fed. R. Evid. 801(d)(2)(D). But the district court did not abuse its discretion in concluding that "[t]he underlying premise that AT&T worked in the capacity of an agent for Defendants is without factual or substantive evidentiary support." ER 19. The supervisor has not offered any testimony, and Klein has no independent basis to report on any alleged relationship between the supervisor and anyone else. Whether the NSA had control and direction over AT&T property and personnel in the SG3 room is precisely the matter plaintiffs seek to prove with

[12] Plaintiffs' reliance (Br. 50, 52) on *United States v. Neal*, 36 F.3d 1190 (1st Cir. 1994) is misplaced. *Neal* held that a bank employee could testify to the contents of business records that she had personally reviewed in the course of performing her assigned duties, not to information told to her by someone else concerning activities with which she was not involved. *Id.* at 1206.

hearsay testimony; plaintiffs cannot bootstrap that hearsay into admissible evidence by pointing only to the hearsay to prove the truth of the matter asserted. Nor can plaintiffs manufacture an agency relationship by noting (Br. 48) that upstream collection under FISA Section 702, where it occurs, involves the compelled assistance of service providers. Even looking past the problem that Section 702 (enacted in 2008) and its directives did not exist at the time of the alleged events in 2002 and 2003, plaintiffs provide no evidence that such a directive or assistance was actually involved here.

Finally, plaintiffs assert (Br. 52-53) that the statements regarding alleged NSA involvement qualify for the exception to the hearsay rule for "[a] statement of the declarant's then-existing state of mind (such as motive, intent, or plan) or emotional, sensory, or physical condition." Fed. R. Evid. 803(3). But none of the statements actually convey an intent *by the out-of-court supervisor* to "meet with the NSA," Br. 52; they offer nothing but a statement that a supposed NSA agent "would … visit" the office, ER 1212.

In any event, Rule 803(3) does not allow hearsay to be used as evidence "to prove the truth of [the] beliefs" conveyed by the out-of-court statement. *Bains v. Cambra*, 204 F.3d 964, 973 (9th Cir. 2000); Fed. R. Evid. 803(3) (disallowing hearsay "statement[s] of memory or belief to prove the fact[s] remembered or believed"). Thus, even if the statements conveyed the intent by AT&T personnel to meet someone, the district court did not abuse its discretion in concluding that those

statements would not be admissible to prove the truth of the supervisor's statement that the person they planned to meet was an NSA agent. *See United States v. Astorga-Torres*, 682 F.2d 1331, 1335 (9th Cir. 1982) ("[A] statement of the declarant's intent to do something is" not admissible "'as (a) narrative() of facts communicated to the (declarant) by others.'" (alterations in original)).

b. Plaintiffs also seek to use Klein's declaration, and a document attached to it, in an attempt to show that the SG3 room contained what plaintiffs' brief calls "spy equipment capable of filtering and searching the copied communications." Br. 40. Attached to Klein's declaration is a document apparently authored by an AT&T Labs consultant, titled "Study Group 3 LGX/Splitter Wiring San Francisco," *see* ER 1282, which, among other things, contains a list of equipment, including something called a "Narus STA 6400." ER 1284. Klein's declaration interprets this as a list of "the equipment installed" in the SG3 room, though he claims no personal knowledge of what was actually installed. ER 1214. And another declarant, Scott Marcus, says that a Narus Semantic Traffic Analyzer is a commercially available device that is "designed to capture data directly from a network," "identify traffic of interest," and "act on it." ER 1053-54. That device could "be used in a number of different ways" by network operators for their own business purposes, ER 1056; *see also* ER 1065-67, but Marcus speculates that this device would be "well suited to the capture and analysis of large volumes of data for purposes of surveillance," ER 1054.

Even if such equipment were in the SG3 room, the presence of commercially available network analysis equipment inside a sophisticated network operator's facility is not evidence that the equipment is being used by the government to facilitate internet content collection, rather than being used by the network operator for any of several business purposes. Factual allegations, like these, that are "merely consistent with" standing or allegedly unlawful conduct are insufficient to withstand a motion to dismiss, *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)—much less a motion for summary judgment. Marcus says that he "can envision no commercial reason" that would make it "likely" that AT&T would have paid "the probable cost" of the equipment purportedly installed in the SG3 room. ER 1045. But Marcus presents no basis for his unspecified cost estimates, and no reasoned explanation of why the numerous other commercial uses for the equipment that Marcus identifies would not justify the expense of the equipment. *See* ER 1065-67. Nor is the bare fact that a cost-justified business rationale is not immediately "apparent" to an outsider like Marcus, ER 1069, material evidence that the government "therefore" must have paid for and operated the equipment for internet content collection, as Marcus asserts, ER 1045. Marcus does not claim personal involvement with, or to be an expert in, AT&T's financial decisionmaking. The district court did not abuse its discretion in concluding that Marcus's "conclusions are not based on sufficient facts or data" regarding how the alleged equipment would have been used. ER 17; *see* Fed. R. Evid. 702.

In any event, plaintiffs failed to muster competent evidence that such equipment was actually in the SG3 room. As the district court correctly held, the document attached to the Klein declaration is hearsay. ER 16. Plaintiffs insist (Br. 48) that the document is not hearsay but rather the statement of the government's agent under Rule 801(d)(2)(D). But, for the same reasons discussed above, plaintiffs have introduced no evidence of such an agency relationship with respect to the equipment or personnel in the SG3 room, or upstream collection more generally. And plaintiffs cannot manufacture such evidence by relying only on the very same evidence that is otherwise inadmissible hearsay. *See* Fed. R. Evid. 801(d)(2) ("The statement must be considered but does not by itself establish … the existence or scope of the relationship under (D).").

Plaintiffs similarly contend (Br. 47-48) that the document qualifies for the state-of-mind exception and is admissible to show intent to install the listed equipment in the SG3 room. But the out-of-court speaker here, according to Klein, is a "consultant" for "AT&T Labs[]," ER 1214, and the document itself, with the word "Study" in the title, ER 1282, makes clear that it is a "first issue" (*i.e.*, with more to come), ER 1283. Plaintiffs present no evidence that this consultant's early stage proposal was ever adopted by AT&T. And, in any event, with no evidence suggesting what was actually installed in the SG3 room, plaintiffs could not hope to leverage evidence of a single consultant's early planning to help show that the listed equipment was later actually installed in the SG3 room—much less that it was used by the NSA.

Finally, for similar reasons, the district court did not abuse its discretion in concluding that the document was not admissible as a business record under Rule 803(6). ER 16. This planning document—dated December 10, 2002, ER 1282, well before the alleged copying and diversion of streams of communications into the SG3 room "[s]tart[ed] in February 2003," ER 1214—is not "[a] record of an act" or "event" that had actually occurred. Fed. R. Evid. 803(6). Plaintiffs cite (Br. 47) *Selig v. United States*, 740 F.2d 572 (7th Cir. 1984), in which a district court admitted a business record created "several months *after*" an event. *Id.* at 578 (emphasis added). But the document here was created well *before* the claimed event occurred, and is thus not a "record" of its occurrence. Moreover, even if a record created well before a supposed event could be thought to be a record of the event itself, plaintiffs cite no authority for the proposition that a court would abuse its discretion in concluding that the substantial gap in time here does not satisfy the rule's requirement that the "record [be] made at or near the time" of the event. Nor do plaintiffs present any admissible evidence that AT&T has ever copied and diverted streams of communications for the NSA or installed and operated NSA surveillance devices for upstream collection—much less evidence that doing so is "a regularly conducted activity of" AT&T. Fed. R. Evid. 803(6)(B). And plaintiffs offer no testimony from a custodian or other "witness knowledgeable about the creation and maintenance of those records," as they must do where the accuracy of the records is at issue. *ABS Entm't, Inc. v. CBS Corp.*, 908 F.3d 405, 426 (9th Cir. 2018). While Klein says that he

"reviewed [the] document", ER 1214-15, he claims no knowledge of the accuracy or reliability of the purported list of equipment inside the SG3 room (which, again, Klein never claims to have seen or used).

3. Plaintiffs are similarly unable (Br. 45-46) to show what equipment was actually installed in the SG3 room using the declaration of AT&T security official James Russell. Russell's declaration supported AT&T's motion in related litigation to compel the return of confidential documents—including the documents attached to Klein's declaration—or maintain the documents under seal. ER 1197. Russell stated that he had "reviewed" the "documents attached to Mr. Klein's declaration," and explained how public disclosure of certain information in those documents could harm AT&T's business interests. ER 1197-98.

Plaintiffs contend that Russell "independently testified" to "the spy equipment in the SG3 room" based on his "personal knowledge of the facts." Br. 45-46. But the district court did not abuse its discretion in concluding otherwise. ER 16. Nothing in the declaration indicates that Russell, a career security officer, ER 1197, had intimate personal knowledge of the variety of extremely technical matters discussed in the underlying documents, including the many specific pieces of equipment at issue. Rather, as the district court reasonably concluded, Russell relied only on the descriptions in the Klein documents and used his personal knowledge of the security threats posed by release of that information, if true, as the basis for his declaration.

4. Plaintiffs' remaining evidence is similarly of no use in establishing standing. Plaintiffs point (Br. 39, 44) to a declaration from another retired AT&T technician, Phillip Long, who states that, while he was stationed at another AT&T facility, he was instructed for reasons he was not told and does not purport to explain "to start rerouting Internet backbone connections through" the Folsom Street facility in San Francisco. ER 957. But the mere fact that these reconfigurations "made no sense *to [Long]*," *id.* (emphasis added), is not evidence that, as plaintiffs insist, they were undertaken "[w]ithout any commercial or engineering purpose," Br. 39, much less evidence that they were undertaken to assist with NSA internet content collection.

Finally, plaintiffs' standing is also unsupported by the declaration of Ashkan Soltani. Soltani states that some "cloud-based [email] applications," such as those subscribed to by plaintiffs, move "shards" of stored emails between data centers "to balance load and in response to failures." ER 996-97. That movement, Soltani concludes, "increases the likelihood" that users' communications will pass through whatever "Internet surveillance collection points" may exist. ER 996. The district court correctly concluded that "[t]his unquantified [increase in the] likelihood of interception regarding some [unspecified] users' email based on the posited Internet surveillance connection points and collection process is insufficient to constitute specific evidence" that *plaintiffs* are among the injured. ER 17. Without evidence of where and how the NSA conducts internet content collection, Soltani's sparse opinion about the unspecified likelihood of collection is not "based on sufficient facts or

data," and the district court did not abuse its discretion in excluding it on that basis. ER 17; *see* Fed. R. Evid. 702(b).

III. Remaining Issues

A. Plaintiffs devote a substantial portion of their opening brief urging the court not only to vacate the district court's judgment concluding that plaintiffs lack standing, but also to decide a question the district court has not yet had an opportunity to address: whether, if plaintiffs have standing to bring a Fourth Amendment challenge to upstream collection, plaintiffs are entitled to summary judgment on the merits of that claim. Br. 64-79. Given the procedural posture, potential remaining threshold issues (such as the statutory privileges invoked by the government), this Court's previous recognition that piecemeal consideration of that particular claim on appeal (separate from the other claims) is not appropriate, and the extraordinary number of issues plaintiffs already call upon this Court to decide in this appeal, this Court should "decline to entertain this constitutional question unnecessarily." *Dorsey v. National Enquirer, Inc.*, 973 F.2d 1431, 1438 (9th Cir. 1992).

B. Plaintiffs also argue that the district court abused its discretion in declining to give plaintiffs' counsel access to the government's classified filings, and, they contend, if this case is remanded for *ex parte* and *in camera* procedures under 50 U.S.C. § 1806(f), "the district court … should be instructed to grant access to cleared plaintiffs' counsel to any classified evidence." Br. 61-62.

There was no abuse of discretion. Plaintiffs' request is extraordinary: As far as we are aware, the government has never been required under 50 U.S.C. § 1806(f), or 18 U.S.C. § 2712(b)(4), to disclose classified information protected by those provisions to any litigant, or litigant's counsel, in any proceeding, civil or criminal—much less the enormous volume of extraordinarily detailed and privileged information at issue here, whose public disclosure would cause exceptionally grave harm to national security. Such disclosure would risk the very type of public disclosure that the state-secrets privilege, and Section 1806(f), are designed to guard against. *See United States v. Daoud*, 755 F.3d 479, 484 (7th Cir. 2014) (unanimously reversing the lone district court order that has granted opposing counsel access to classified information under Section 1806(f), and observing that even "cleared lawyers" might, "in their zeal to defend their client," or "misremembering what is classified and what not, inadvertently say things that would provide clues to classified material").

Plaintiffs' request for such extraordinary, and dangerous, access is not "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Plaintiffs' bald assertion that the district court "lacked the time, resources, and technical background to analyze" the *ex parte* filings, or was hampered by the manner in which those filings were presented, Br. 61, is belied by the record. *See* ER 29 ("The Court has diligently reviewed the materials submitted …. Although the Government's substantive responses … are organized thematically and by category, the Court finds that … the Government has fully and fairly complied with

the Court's instructions."). And the small number of instances plaintiffs point to, in which the government has, on its own, identified and corrected unintentional errors in communications with the FISC and the district court, *see* Br. 62, only underscore the seriousness with which the government takes its duty of candor.

Plaintiffs' unelaborated assertion that being denied access "deprived plaintiffs of due process"—made in a single sentence with no citation to any authority, Br. 62—is not only forfeited but also foreclosed by binding circuit precedent. *Fazaga*, 916 F.3d at 1226 ("As it is Plaintiffs who have invoked the FISA procedures, we proceed on the understanding that they are willing to accept those restrictions."); *Ott*, 827 F.2d at 477 (denying access to *ex parte* and *in camera* materials under Section 1806(f) in court-martial proceedings did not deprive service member of due process).

CONCLUSION

For the foregoing reasons, the judgment of the district court should be affirmed.

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

H. THOMAS BYRON III
s/ Joseph F. Busa
JOSEPH F. BUSA
Attorneys, Appellate Staff
Civil Division, Room 7537
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 305-1754
Joseph.F.Busa@usdoj.gov

December 2019

STATEMENT OF RELATED CASES

Appellees know of no related case pending in this Court. *See* Ninth Circuit Rule 28-2.6.

s/ Joseph F. Busa
Joseph F. Busa
Counsel for Appellees

CERTIFICATE OF COMPLIANCE (FORM 8)

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 17,531 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:

[ ] 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:
- [ ] 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/ Joseph F. Busa* **Date**: December 6, 2019

ADDENDUM

TABLE OF CONTENTS

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

(a) In General.—

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

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.—

. . .

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) [*i.e.*, 50 U.S.C. §§ 1806(f), 1825(g), 1845(f)] shall be the exclusive means by which materials governed by those sections may be reviewed.

. . .

Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.*

§ 1801. Definitions

. . .

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

. . .

§ 1806. Use of information

. . .

(c) Notification by United States. Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

. . .

(e) Motion to suppress. Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that—

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders. Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

. . .