
NATIONAL SECURITY — SURVEILLANCE — NINTH CIRCUIT
HOLDS THAT FISA DISPLACES THE STATE SECRETS PRIVILEGE
FOR ELECTRONIC SURVEILLANCE. — *Fazaga v. FBI*, 916 F.3d 1202
(9th Cir. 2019).

The state secrets privilege is an evidentiary privilege pursuant to which the executive branch can seek to remove evidence from litigation because it could endanger national security if made public. Announced in the 1953 case *United States v. Reynolds*,¹ the modern privilege is strong medicine: if the government convinces a court that evidence poses a “reasonable danger” to national security, the court must exclude it,² even if doing so means the court must dismiss the case.³ Twenty-five years after *Reynolds*, Congress enacted the Foreign Intelligence Surveillance Act of 1978⁴ (FISA), a statutory scheme that establishes electronic surveillance policies, provides a private right of action to challenge unlawful surveillance,⁵ and creates procedures, codified in 50 U.S.C. § 1806(f), that govern the review of classified material in the electronic surveillance context.⁶ Recently, in *Fazaga v. FBI*,⁷ the Ninth Circuit became the first court of appeals to hold that, with respect to electronic surveillance, § 1806(f) displaced the state secrets privilege and its dismissal remedy.⁸ While reactions to *Fazaga* suggest that it broke significant new ground in surveillance litigation, in reality it likely did not, given the threshold barriers that will generally prevent litigants from ever reaching the door it opened.

The Ninth Circuit had occasion to consider § 1806(f)’s relationship to the *Reynolds* privilege because of a fitness instructor named Craig Monteilh and the counterterrorism operation named in his honor: Operation Flex.⁹ In 2006, the FBI launched Operation Flex and recruited Monteilh to be an informant.¹⁰ At the FBI’s direction, Monteilh pretended to convert to Islam and joined a mosque, the Islamic Center of Irvine (ICOI), where he collected information about its attendees and

¹ 345 U.S. 1 (1953).

² *Id.* at 10. There is another strand of the privilege, recognized in *Totten v. United States*, 92 U.S. 105, 107 (1876), but it is not relevant to this discussion.

³ See, e.g., Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1262–63 (2007).

⁴ Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

⁵ 50 U.S.C. § 1810 (2012).

⁶ *Id.* § 1806(f).

⁷ 916 F.3d 1202 (9th Cir. 2019).

⁸ *Id.* at 1211.

⁹ Class Action Complaint at 24, *Fazaga v. FBI*, 884 F. Supp. 2d 1022 (C.D. Cal. 2012) (No. 11-cv-00301). Given the procedural posture of the case, the Ninth Circuit took all facts as alleged by the plaintiffs. *Fazaga*, 916 F.3d at 1211. This analysis does likewise.

¹⁰ *Fazaga*, 916 F.3d at 1212.

other local Muslims.¹¹ Monteilh spent more than a year in this role, during which time he wore a wire, planted recording devices in mosques, and passed information to the FBI.¹² The FBI also installed surveillance devices at ICOI and several other mosques, as well as in the homes, offices, and cars of several ICOI congregants.¹³ The FBI eventually lost confidence in Monteilh and dismissed him.¹⁴ Operation Flex came to light several years later during the naturalization fraud prosecution of an ICOI member.¹⁵ An FBI agent testified about recordings that an informant created, and the context revealed that the informant was Monteilh.¹⁶ Both the FBI and Monteilh subsequently confirmed the operation and the use of electronic surveillance.¹⁷

Three Muslims with whom Monteilh had interacted filed suit against the FBI, the United States, two FBI officials in their official capacities, and five FBI agents in their individual capacities.¹⁸ The plaintiffs sought damages and injunctive relief through the destruction of records the FBI may have illegally obtained.¹⁹ They asserted eleven causes of action, some for violations of the First Amendment, the Fifth Amendment, the Religious Freedom Restoration Act of 1993²⁰ (RFRA), the Federal Tort Claims Act²¹ (FTCA), and the Privacy Act of 1974²² (collectively, the discrimination claims²³), as well as others for violations of the Fourth Amendment and FISA (collectively, the surveillance violation claims).²⁴ The defendants moved to dismiss.²⁵ The government specifically argued that the discrimination claims should be dismissed under the state secrets privilege and proffered documents asserting that these claims could not be litigated without undue risk to national security.²⁶ Relying on these documents, the district court dismissed not only the discrimination claims but also all of the non-FISA claims under the state secrets privilege, explaining that the government could not defend itself without “rely[ing] on . . . privileged material.”²⁷ The court also

¹¹ *Id.*

¹² *Id.* at 1212–13.

¹³ *Id.* at 1213, 1218.

¹⁴ *Id.* at 1214.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.* at 1210.

¹⁹ *Id.* at 1214, 1235.

²⁰ 42 U.S.C. §§ 2000bb to 2000bb-4 (2012).

²¹ 28 U.S.C. § 1346(b) (2018).

²² 5 U.S.C. § 552a (2018).

²³ In effect, these claims assert that the plaintiffs were surveilled because they were Muslims.

²⁴ *Fazaga*, 916 F.3d at 1214.

²⁵ The individual defendants claimed qualified immunity and the government argued that the surveillance violation claims failed for a variety of reasons. *Id.* at 1214–15.

²⁶ *Id.* at 1215.

²⁷ *Id.*

dismissed the FISA claim against the government but allowed the FISA claim against the individual defendants to proceed.²⁸

The Ninth Circuit affirmed in part and reversed in part.²⁹ Writing for the panel, Judge Berzon³⁰ first addressed the FISA claim against the individual defendants — the only claim the district court did not dismiss. She held that the defendants were entitled to qualified immunity with respect to certain acts of surveillance³¹ but were not with respect to recordings taken in the plaintiffs’ homes and offices,³² because these recordings “violated . . . statutory or constitutional right[s]” that were “clearly established” at the time of the violations.³³

The court next concluded that the district court erred by dismissing the Fourth Amendment claims under the state secrets privilege, because the privilege only applies to claims for which the government invokes it, and the government only did so for the discrimination claims.³⁴ More broadly, the court held that, where they apply, § 1806(f)’s procedures displace the state secrets privilege with respect to electronic surveillance.³⁵ For § 1806(f) to apply, the government must attempt to “use” information obtained through electronic surveillance against an “aggrieved person” in a judicial proceeding or an aggrieved person must seek to “discover or obtain” such materials.³⁶ Judge Berzon found that these conditions were met, so the district court should have followed § 1806(f) and evaluated the classified material in camera and ex parte to assess whether the FBI surveilled the plaintiffs because of their religion and thus violated the Constitution instead of dismissing the discrimination claims on the basis of the state secrets privilege.³⁷

The court then held that the First, Fourth, and Fifth Amendment claims against the official capacity defendants and the Establishment

²⁸ *Id.*

²⁹ *Id.* at 1254.

³⁰ Judge Berzon was joined by Judge Gould and Judge Steeh. Judge Steeh, from the Eastern District of Michigan, sat by designation.

³¹ Specifically, the defendants enjoyed qualified immunity for the recordings of conversations in which Monteilh took part and recordings from devices Monteilh hid inside mosques. *Fazaga*, 916 F.3d at 1219–24.

³² *Id.* at 1225.

³³ *Id.* at 1217 (quoting *Ashcroft v. al-Kidd*, 563 U.S. 731, 735 (2011)). The panel only allowed the claim for this category of surveillance to proceed against two of the individual defendants, as the plaintiffs failed to plausibly allege that the other three were involved. *Id.* at 1225.

³⁴ *Id.* at 1228.

³⁵ *Id.* at 1231–34.

³⁶ *Id.* at 1234 (first quoting 50 U.S.C. § 1801(c) (2012); then quoting *id.* § 1801(f); and then quoting *id.*); see *id.* at 1235; see also 50 U.S.C. § 1801(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.”). There is another path to § 1806(f) not addressed in this case, which is triggered when an aggrieved person motions to suppress evidence obtained through FISA. 50 U.S.C. § 1806(f).

³⁷ *Fazaga*, 916 F.3d at 1231 (quoting 50 U.S.C. § 1806(f)); see also *id.* at 1235.

Clause and Fifth Amendment equal protection *Bivens*³⁸ claims against the individual defendants could proceed but dismissed the other *Bivens* claims because alternative remedies for the alleged violations precluded *Bivens* redress.³⁹ The court also found that the individual defendants were entitled to qualified immunity for RFRA claims but that RFRA claims against the government could proceed.⁴⁰ Finally, the court dismissed the 42 U.S.C. § 1985(3) constitutional claims⁴¹ and the Privacy Act claim⁴² and allowed the FTCA claim to proceed.⁴³ All told, the panel reversed all state secrets–based dismissals, dismissed several claims on other grounds, and allowed a number of claims to proceed.

Judge Berzon’s holding that FISA abrogates the state secrets privilege with respect to electronic surveillance weakened one of the primary tools the government uses to counter challenges to its surveillance practices. Reactions to *Fazaga* suggest that this will have a significant impact on future surveillance litigation. But there are strong reasons to believe that few litigants will ever be able to take advantage of *Fazaga*. Before a litigant can reach § 1806(f)’s procedures, she must: (a) learn that she was surveilled; (b) establish standing; and (c) prove that she is an “aggrieved person” within the meaning of FISA. Jumping over these cumulative hurdles will be difficult, and few litigants are likely to succeed, not least because even after *Fazaga*, the government can invoke the state secrets privilege to prevent plaintiffs from doing so. As a result, *Fazaga*’s impact will probably be modest at best.

Civil liberties advocates and the government alike have described *Fazaga* as potentially groundbreaking. The ACLU applauded the decision as “a landmark victory for freedom of religion and human rights.”⁴⁴ The Electronic Frontier Foundation (EFF) suggested that after *Fazaga*, “the government can no longer rely on blanket secrecy claims to keep courts from ruling on illegal surveillance.”⁴⁵ The FBI promptly sought

³⁸ *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). A *Bivens* claim is a claim against federal officers seeking damages directly under the Constitution. See Gene R. Nichol, *Bivens, Chilicky, and Constitutional Damages Claims*, 75 VA. L. REV. 1117, 1118 n.3 (1989). *Bivens* claims have been limited where Congress has provided alternative remedies for the alleged violations. See, e.g., *Wilkie v. Robbins*, 551 U.S. 537, 562 (2007); *Bush v. Lucas*, 462 U.S. 367, 368 (1983).

³⁹ *Fazaga*, 916 F.3d at 1241–43.

⁴⁰ *Id.* at 1248.

⁴¹ *Id.* at 1246. The court held that the defendants against whom the claims were asserted were entitled to qualified immunity. *Id.*

⁴² *Id.* at 1249. The court held that the Privacy Act barred the relief the plaintiffs sought. *Id.*

⁴³ *Id.* at 1250–51. The court concluded that resolution of the claim would likely “turn on the district court’s ultimate resolution of the merits of Plaintiffs’ various federal constitutional and statutory claims,” and therefore addressing it was premature. *Id.* at 1251.

⁴⁴ Press Release, ACLU of S. Cal., Landmark Legal Ruling Permits Courts to Review Claims of Unlawful Surveillance of Muslims (Feb. 28, 2019), <https://www.aclusocal.org/en/press-releases/landmark-legal-ruling-permits-courts-review-claims-unlawful-surveillance-muslims> [https://perma.cc/GSW3-2Y9Q].

⁴⁵ Elec. Frontier Found. (@EFF), TWITTER (Feb. 28, 2019, 3:57 PM), <https://twitter.com/EFF/status/1101224838566313984> [https://perma.cc/V8VA-3WTP].

rehearing en banc, stating in its petition that the ruling portended “potentially grave consequences for the Executive Branch’s ability to protect state secrets and the national security.”⁴⁶ Both the government and civil libertarians are likely looking ahead to what *Fazaga* could mean for other cases, particularly challenges to NSA mass surveillance programs.⁴⁷ EFF tweeted that *Fazaga* “potentially remov[ed] one of the roadblocks . . . in [its] NSA surveillance litigation,”⁴⁸ and within seven months the ACLU,⁴⁹ the Knight First Amendment Institute,⁵⁰ the Center for Democracy and Technology,⁵¹ and EFF⁵² all cited *Fazaga* extensively in cases challenging government surveillance.

Observers likely reacted as they did because, by replacing the state secrets privilege with § 1806(f), the Ninth Circuit potentially left the government more vulnerable to challenges to its surveillance practices. Both § 1806(f) and state secrets review allow judges to review classified information under some circumstances.⁵³ A judge reviewing material under § 1806(f) assesses “whether the surveillance of the aggrieved person was *lawfully authorized and conducted*.”⁵⁴ By contrast, a judge’s review of evidence over which the state secrets privilege has been asserted evaluates whether compelling the evidence would pose a “reasonable danger” to national security.⁵⁵ If it would, the privilege absolutely bars the information from disclosure, *even if that information discloses government wrongdoing*.⁵⁶ Thus in a case where information that poses

⁴⁶ Petition for Rehearing or Rehearing En Banc at 1, *Fazaga*, 916 F.3d 1202 (Nos. 12-56867, 12-56874, 13-55017).

⁴⁷ Since at least the early 2000s, the NSA has engaged in various forms of bulk electronic surveillance, the legal authority and status of which have been contested and frequently in flux. *See generally* CHARLIE SAVAGE, *POWER WARS* 162–223, 555–626 (rev. ed. 2017) (discussing the NSA’s electronic surveillance programs).

⁴⁸ Elec. Frontier Found., *supra* note 45; *see also* Cindy Cohn & Karen Gullo, *Government Fights to Trap EFF’s NSA Spying Case in a Catch-22*, ELECTRONIC FRONTIER FOUND. (Apr. 11, 2019), <https://www.eff.org/deeplinks/2019/04/government-fights-trap-effs-nsa-spying-case-catch-22> [https://perma.cc/F3QG-KGEP] (calling *Fazaga* a “boost” to EFF’s case versus the NSA).

⁴⁹ *See, e.g.*, [Proposed] Brief of Amici Curiae the American Civil Liberties Union et al. in Support of Twitter, Inc.’s Opposition to Defendants’ Invocation of State Secrets and Motion to Dismiss at 9–11, *Twitter, Inc. v. Barr*, No. 14-cv-04480 (N.D. Cal. May 6, 2019).

⁵⁰ Plaintiff Wikimedia Foundation’s Sur-reply in Opposition to Defendants’ Motion for Summary Judgment at 14–15, *Wikimedia Found. v. NSA*, No. 15-cv-00662 (D. Md. Dec. 16, 2019).

⁵¹ Brief of Center for Democracy and Technology and New America’s Open Technology Institute as Amici Curiae in Support of Plaintiffs-Appellants and in Support of Reversal at 18, *Jewel v. NSA*, No. 19-16066 (9th Cir. Sept. 13, 2019).

⁵² Appellants’ Opening Brief at 21–23, *Jewel*, No. 19-16066 (Sept. 10, 2019).

⁵³ *Compare* 50 U.S.C. § 1806(f) (2012) (“[T]he . . . court . . . shall . . . review in camera and ex parte the [FISA] application, order, and such other materials relating to the surveillance as may be necessary . . .”), *with* Chesney, *supra* note 3, at 1252 (explaining that under *Reynolds*, “the court can personally review the sensitive information on an *in camera*, ex parte basis if necessary”).

⁵⁴ 50 U.S.C. § 1806(f) (emphasis added).

⁵⁵ *United States v. Reynolds*, 345 U.S. 1, 10 (1953); *see id.* at 9; Chesney, *supra* note 3, at 1286–87.

⁵⁶ *See El-Masri v. United States*, 479 F.3d 296, 306 (4th Cir. 2007).

a danger to national security also reveals unlawful surveillance, FISA provides an opportunity for meritorious claims to survive that the state secrets privilege would have foreclosed.

But other obstacles may well prevent most potential plaintiffs from capitalizing on *Fazaga*. The first of these is learning that one may have been surveilled. But for an incidental revelation, no one would have known about Operation Flex.⁵⁷ Because FISA does not require that notice be provided to surveillance targets (outside of a few limited contexts),⁵⁸ only in similar cases of mistake or leak will those who have been unlawfully surveilled have any inkling that their rights were violated. *Fazaga* did not alter FISA's notice regime, and thus most surveillance violations will remain out of court and not subject to § 1806(f) review.⁵⁹

Should someone learn enough to suspect that the government illegally surveilled her, she has another threshold problem: standing. Article III requires that plaintiffs have a particularized "injury in fact" that is "fairly . . . trace[able]" to the challenged conduct and that the case has some likelihood of redressing.⁶⁰ Meeting these criteria may be difficult even for those who are aware that they were likely surveilled. For example, in *ACLU v. NSA*,⁶¹ U.S. residents who communicated electronically with suspected al Qaeda affiliates abroad challenged a publicly acknowledged program under which the government intercepted, without a warrant, electronic communications in which one party was a suspected al Qaeda affiliate located overseas.⁶² But, although the plaintiffs had every reason to suspect their communications had been intercepted, they lacked "evidence that [they] *themselves* ha[d] been [surveilled],"⁶³ and the case was dismissed for lack of standing.⁶⁴ In *Fazaga*, by contrast, standing was no issue. The FBI

⁵⁷ *Fazaga*, 916 F.3d at 1214.

⁵⁸ FISA provides for notice in three scenarios. The first is when the government seeks to introduce electronic surveillance evidence in a criminal prosecution. 50 U.S.C. § 1806(c)–(d). The second applies only to physical searches. *Id.* § 1825(b). The final notice provision applies only in emergencies where the Attorney General authorizes a search before getting Foreign Intelligence Surveillance Court (the court whose authorization is required for electronic surveillance) approval. *Id.* § 1805(e). In such cases, the government must seek ex post approval, and if approval is denied, notification may be required. *Id.* § 1806(j); see also Andrew Adler, Note, *The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act*, 61 U. MIAMI L. REV. 393, 403–07 (2007).

⁵⁹ In *In re NSA Telecommunications Records Litigation*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008), the district court predicted this dynamic, holding that FISA displaced the state secrets privilege but noting that notice and the aggrieved person requirement "make section 1810 a mostly theoretical, but rarely, if ever, a practical vehicle for seeking a civil remedy for unlawful surveillance." *Id.* at 1125.

⁶⁰ *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (alteration and omission in original) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41 (1976)); see *id.* at 561.

⁶¹ 493 F.3d 644 (6th Cir. 2007).

⁶² *Id.* at 648–49.

⁶³ *Id.* at 673 (emphasis added).

⁶⁴ *Id.* at 688–89. The Supreme Court reached the same result on similar facts in *Clapper v. Amnesty International USA*, 568 U.S. 398, 402 (2013). By contrast, in *Wikimedia Foundation v. NSA*, 857 F.3d

accidentally revealed that it had surveilled the plaintiffs.⁶⁵ Absent such circumstances, litigants are likely to be able to show only a *possibility* that they were surveilled, which to date has had little traction in court.

Moreover, even after *Fazaga*, the government appears to be able to invoke the state secrets privilege to withhold evidence that might help plaintiffs establish standing. In *Jewel v. NSA*,⁶⁶ the first case since *Fazaga* in which a court bound by the holding considered a challenge to secret electronic surveillance, this is exactly what happened. The *Jewel* court found that the NSA properly invoked the state secrets privilege over evidence indicating whether the plaintiffs had been surveilled and granted the NSA's motion for summary judgment, never reaching § 1806(f) review.⁶⁷ If *Jewel* is indicative, *Fazaga* may only be impactful in cases where plaintiffs acquire meaningful proof of their surveillance, something the state secrets privilege can still prevent.⁶⁸

Fazaga also did nothing to help plaintiffs establish aggrieved-person status under FISA, a further prerequisite to § 1806(f) review. Establishing aggrieved-person status means proving that one was “the target of” or “subject to” electronic surveillance.⁶⁹ Some courts treat aggrieved-person status as identical to standing, but others consider it to require a stronger evidentiary showing of the facts that tend to establish standing.⁷⁰ Either way, Judge Berzon made clear that for § 1806(f) to apply, a plaintiff “*must* satisfy the definition of an ‘aggrieved person,’”⁷¹ and § 1806(f) is unambiguous about the fact that only when the government seeks to introduce evidence against an aggrieved person or when an aggrieved person requests FISA material may the court review such

193 (4th Cir. 2017), the court held that Wikimedia established standing sufficient to survive a motion to dismiss because, given the breadth of the NSA's surveillance and the “volume of Wikimedia's communications,” it was plausible that the NSA had intercepted Wikimedia's information. *Id.* at 210. The court distinguished *Clapper* in part because *Clapper* was decided at summary judgment and “what may perhaps be speculative at summary judgment can be plausible on a motion to dismiss.” *Id.* at 212.

⁶⁵ *Fazaga*, 916 F.3d at 1214.

⁶⁶ No. C 08-04373, 2019 U.S. Dist. LEXIS 217140 (N.D. Cal. Apr. 25, 2019).

⁶⁷ *Id.* at *49-50.

⁶⁸ For a discussion of potential solutions to the standing and state secrets doom loop, see Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 *IS* 551, 567-678 (2014).

⁶⁹ 50 U.S.C. § 1801(k) (2012).

⁷⁰ FISA's legislative history suggests that Congress intended aggrieved-person status to be “co-extensive” with Fourth Amendment standing under *Alderman v. United States*, 394 U.S. 165 (1969). H.R. REP. NO. 95-1283, pt. 1, at 66 (1978). By contrast, some courts have collapsed the aggrieved-person and Article III standing inquiries. See, e.g., *ACLU v. NSA*, 493 F.3d 644, 683 (6th Cir. 2007). Other courts have treated the aggrieved-person inquiry as separate and only relevant after standing is established. See *Jewel v. NSA*, 673 F.3d 902, 907 n.4 (9th Cir. 2011) (stating that whether a plaintiff is an aggrieved person is a “merits determination, not a threshold standing question”); *Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 786 (D. Md. 2018) (holding that although a plaintiff had demonstrated standing sufficient to survive a motion to dismiss, it had not shown that it was an “aggrieved person” that could avail itself of § 1806(f)).

⁷¹ *Fazaga*, 916 F.3d at 1238 (emphasis added) (quoting 50 U.S.C. § 1801(k)).

material.⁷² The information that established the *Fazaga* plaintiffs' standing — the FBI's and Monteilh's admissions — also allowed them to show that they were aggrieved persons.⁷³ There is no reason to expect that many plaintiffs will acquire such probative evidence.⁷⁴

Jewel supports a narrow reading of *Fazaga* with respect to aggrieved-person status determination. The *Jewel* court held that § 1806(f) only abrogates the state secrets privilege once plaintiffs establish that surveillance took place, and the state secrets privilege is still available to prevent plaintiffs from doing so.⁷⁵ On appeal, the plaintiffs have argued that, because the *Fazaga* court ordered § 1806(f) review where aggrieved-person status had only been alleged, well-pleaded allegations of surveillance should always lead to such review.⁷⁶ But in *Fazaga*, which was considered at the motion to dismiss stage, the Ninth Circuit noted that the allegations were "sufficient *if proven* to establish that Plaintiffs are 'aggrieved persons.'" ⁷⁷ This language suggests that plaintiffs need to prove such status, not just allege it. Further, in *Fazaga* the court "was not presented with the issue of what to do [where a plaintiff's status as an aggrieved person] . . . is the very information over which the Government seeks to assert the state secrets privilege."⁷⁸ Unless and until the Ninth Circuit holds either that plaintiffs can overcome government contestation of aggrieved-person status with mere allegations or that the state secrets privilege cannot be invoked to dispute aggrieved-person status, *Fazaga* will likely be limited.

The current state of affairs is unsatisfying no matter where one sits. Despite positive reactions from the plaintiffs' bar, *Fazaga* is unlikely to open the floodgates for even meritorious challenges to electronic surveillance. *Jewel* illustrates the state of play: *Fazaga* purported to displace the state secrets privilege, yet the state secrets privilege continues to preclude the plaintiffs from taking advantage of *Fazaga*. The government's petition for *Fazaga*'s rehearing en banc suggests that it is also displeased, and that in its view the panel extended FISA to a domain in which it was never meant to operate. Perhaps both sides would agree that there must be a better way to litigate electronic surveillance in the twenty-first century. There probably is, but *Fazaga* did not provide it.

⁷² See 50 U.S.C. § 1806(f).

⁷³ See *Fazaga*, 916 F.3d at 1238–39.

⁷⁴ See Adler, *supra* note 58, at 397–98.

⁷⁵ *Jewel v. NSA*, No. C 08-04373, 2019 U.S. Dist. LEXIS 217140, at *46–49 (N.D. Cal. Apr. 25, 2019).

⁷⁶ Appellants' Opening Brief, *supra* note 52, at 21–23.

⁷⁷ *Fazaga*, 916 F.3d at 1216 (emphasis added) (quoting 50 U.S.C. § 1801(k)); see also *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 469 (D.C. Cir. 1991) (suggesting that plaintiffs must raise a genuine dispute of material fact as to their aggrieved-person status before a court assesses whether electronic surveillance was lawful); *Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 780 (D. Md. 2018) (holding that a plaintiff cannot reach § 1806(f) without "adduc[ing] evidence that it has been the subject of electronic surveillance").

⁷⁸ *Jewel*, 2019 U.S. Dist. LEXIS 217140, at *47.