COMMENTS

PIERCING THE VEIL: RECONCILING FISA AND THE STATE SECRETS PRIVILEGE IN THE *SCHREMS II* ERA

CHRIS BAUMOHL*

Twenty years after 9/11 and the beginning of the "War on Terror," access to judicial redress arising out of national security programs remains mired in a labyrinth of procedural hurdles, including the state secrets privilege. Nearly seventy years after the Supreme Court first enunciated the modern state secrets privilege, courts still struggle to articulate a practicable standard that appropriately balances the government's need to protect its secrets and plaintiffs' need to vindicate their constitutional rights. This issue is particularly acute in surveillance litigation, where broad construction of the privilege precludes plaintiffs from establishing standing. However, as the Ninth Circuit found in Fazaga v. FBI*, the Foreign Intelligence Surveillance Act (FISA) empowers courts to determine the lawfulness of electronic surveillance through its* in camera, ex parte *procedures.*

This Comment argues that FISA's procedures displace the state secrets privilege in electronic surveillance cases, even where the government invokes the privilege to protect evidence regarding whether a particular plaintiff was subject to surveillance and thus an "aggrieved person" under FISA. In doing so, this Comment traces the development of post-9/11 surveillance litigation and the

* Senior Staff Member, *American University Law Review*, Volume 71; J.D./M.A. Candidate, May 2022, *American University Washington College of Law*; B.A., *Tufts University*, 2014. I would like to thank the entire *American University Law Review* team for their work in preparing this piece for publication. I am deeply grateful to my advisor, Professor Alex Joel, who challenged me to make the most persuasive argument possible. I am also eternally grateful to my partner, Leah, and my family for their support.

current split over FISA preemption. This Comment then compares the Ninth Circuit's findings in Fazaga *to two National Security Agency (NSA) surveillance cases: the Fourth Circuit's decision in* Wikimedia Foundation v. NSA, *in which it rejected a similar preemption argument in a challenge to NSA surveillance; and the Ninth Circuit's decision in* Jewel v. NSA, *in which it upheld a district court dismissal on state secrets grounds after an exhaustive* in camera, ex parte *review of classified documents. This Comment argues that the district court in* Jewel *correctly undertook* in camera *review because FISA's procedures apply even where the government's invocation of the privilege cuts to the plaintiff's status as an aggrieved person. This Comment then concludes by linking these challenges to NSA surveillance programs to the ongoing privacy debate between the European Union and United States. In particular, it argues that the Court of Justice for the European Union's decision in* Schrems II, *which struck down the E.U.-U.S. Privacy Shield Framework, underscores the continued importance of mechanisms for judicial redress in electronic surveillance cases in aligning the United States and European Union on data privacy.*

*While FISA's procedures remain secretive and deferential to the government, they offer an important opportunity for redress for surveillance abuses. By using § 1806(f)'s procedures, plaintiffs have greater actionable rights in U.S. courts, which may bring the United States into greater alignment with Europe on data protection and redress for surveillance abuses. As the Supreme Court prepares to decide the first two state secrets cases arising out of post-9/11 national security programs—*Fazaga *and* United States v. Zubaydah*—further engagement around this topic is necessary to strike the proper balance between government secrecy and redress.*

TABLE OF CONTENTS

INTRODUCTION

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the E.U.-U.S. Privacy Shield program in *Data Protection Commissioner v. Facebook Ireland Ltd.*[1] (*Schrems II*), in part because the CJEU found that the current legal framework for electronic surveillance[2] in the United States does not offer parties actionable

1. Case C-311/18, ECLI:EU:C:2020:559 (July 16, 2020).

2. The Foreign Intelligence Surveillance Act defines four categories of "electronic surveillance": (1) the electronic acquisition of radio or wire

rights in U.S. courts to redress harms resulting from the government's infringement on data privacy.[3] *Schrems II* is the latest development in a decades-long conflict between the United States and European Union over the availability of individual redress for privacy and data protection violations.[4]

The response from the United States has been marked with frustration and even outright incredulity.[5] The U.S. government, for its part, faulted the CJEU for overlooking various avenues for redress available in Article III courts.[6] In particular, the U.S. government

---

communications by a U.S. person who is in the United States under circumstances in which a warrant would generally be required for law enforcement purposes; (2) the electronic acquisition of the contents of any wire communication to or from a person in the United States, without consent of either party involved; (3) the intentional electronic acquisition of the contents of any radio communication between parties all within the United States, under circumstances in which a warrant would be required for law enforcement purposes; and (4) the installation or use of surveillance technology in the United States to acquire information, other than from a wire or radio communication, under circumstances in which a warrant would be required for law enforcement purposes. 50 U.S.C. § 1801(f). The NSA defines its activities as "signals intelligence," which "involves collecting foreign intelligence from communications and information systems," but this Comment will use "electronic surveillance" throughout for consistency. *See Frequently Asked Question (FAQ)*, NAT'L SEC. AGENCY/CENT. SEC. SERV., https://www.nsa.gov/about/faqs/sigint-faqs [https://perma.cc/EZJ5-T3KW] (defining signals intelligence).

3. *Id.* at ¶¶ 178–85. The Privacy Shield program was the latest framework designed by U.S., E.U., and Swiss authorities to provide a mechanism by which U.S., E.U., and Swiss companies could comply with data protection requirements when transferring personal data across the Atlantic. Privacy Shield Framework, Privacy Shield Overview, https://www.privacyshield.gov/Program-Overview [https://perma.cc/H9B5-WHXG].

4. Christopher Docksey, Schrems II *and Individual Redress—Where There's a Will, There's a Way*, LAWFARE (Oct. 12, 2020, 10:40 AM), https://www.lawfareblog.com/schrems-ii-and-individual-redress-where-theres-will-theres-way [https://perma.cc/84EH-JSQ4] (observing that the CJEU previously rejected the U.S. Safe Harbor law (*Schrems I*) and set aside laws and treaties from other nations for failing to respect privacy rights embodied in the EU Charter of Fundamental Rights).

5. *See, e.g.*, Stewart Baker, *How Can the U.S. Respond to* Schrems II*?*, LAWFARE (July 21, 2020, 8:11 AM), https://www.lawfareblog.com/how-can-us-respond-schrems-ii [https://perma.cc/5XCM-LKBP] (arguing that the *Schrems II* decision is "gobsmacking in its mix of judicial imperialism and Eurocentric hypocrisy" because the CJEU and European Union "have no authority to elaborate or enforce these rights against any of the EU's member states").

6. *See* U.S. DEP'T OF COM., INFORMATION ON U.S. PRIVACY SAFEGUARDS RELEVANT TO SCCS AND OTHER EU LEGAL BASES FOR EU-U.S. DATA TRANSFERS AFTER *SCHREMS II* 12 (2020), https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF [https://perma.cc/7FEU-988N]

mentioned one case—*Wikimedia Foundation v. NSA*[7]—as evidence that a plaintiff could theoretically seek redress by challenging the legality of certain surveillance programs.[8] However, in practice, Wikimedia and other plaintiffs have struggled to clear the myriad procedural obstacles to redress for unlawful surveillance, raising the question of whether this avenue for redress is merely illusory.[9] The CJEU emphasized some of these obstacles, particularly for non-U.S. persons; however, it failed to address a particularly important judicially created obstacle—the state secrets privilege. This privilege, which allows the U.S. government to prevent the release of information that could harm national security, has long stymied efforts for redress in electronic surveillance and other national security litigation.[10]

The E.U.-U.S. debate over privacy and redress comes at a broader inflection point for the United States. The 9/11 terrorist attacks indelibly shaped U.S. foreign affairs and national security policy, spurring the so-called "War on Terror." According to critics, the War on Terror also enabled expansive executive power, excessive secrecy, and inadequate oversight, which in turn have resulted in overreaching and harmful actions and policies.[11] Now, twenty years later, American leaders—including President Biden and his administration—have signaled that they intend to close the post-9/11 era of American

---

(highlighting three U.S. statutes that provide redress to individuals that *Schrems II* did not address).

7. 857 F.3d 193 (4th Cir. 2017).

8. U.S. DEP'T OF COM., *supra* note 6, at 13 & n.45. Wikimedia, the operator of Wikipedia, has challenged the constitutionality of an NSA electronic surveillance program under the First and Fourth Amendments. *Wikimedia*, 857 F.3d at 202.

9. *See infra* Section I.A.5 (discussing the most recent challenges to NSA surveillance programs).

10. *See* Stephen I. Vladeck, *The Demise of Merits-Based Adjudication in Post-9/11 National Security Litigation*, 64 DRAKE L. REV. 1035, 1066–67 (2016) (noting that the privilege has figured prominently in post-9/11 civil litigation); *infra* Section I.C (explaining the state secrets privilege in detail).

11. *See* Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69, 71 (2015) (emphasizing that the post-9/11 decision making under both the Bush and Obama Administrations featured expansive executive power, excessive secrecy, and inadequate oversight, particularly in the context of electronic surveillance). *See generally* SPENCER ACKERMAN, REIGN OF TERROR: HOW THE 9/11 ERA DESTABILIZED AMERICA AND PRODUCED TRUMP (2021) (arguing that War on Terror policies—including surveillance, detention, immigration restrictions, and the use of military force abroad—fed nativist political movements and paved the way for the deployment of some of the same counterterrorism architecture domestically).

history.[12] However, notably missing from the official discourse surrounding the post-9/11 era's legacy is any emphasis on providing redress for those affected. Indeed, to the highly secretive nature of U.S. intelligence programs, attempts to seek judicial redress have often proven impossible without the government's admission of information or a leak.[13] This is precisely the issue for plaintiffs like Wikimedia.

However, just as the CJEU handed down the *Schrems II* decision, the Ninth Circuit preserved hope for surveillance redress. In *Fazaga v. FBI*,[14] three Muslim men alleged that the FBI conducted surveillance on them and their community through a paid confidential informant and electronic surveillance.[15] Although the FBI had disclosed some

---

12. After campaigning on a platform to "end the forever wars" born out of 9/11, President Biden has taken steps to end some of the United States' ground wars. THE POWER OF AMERICA'S EXAMPLE: THE BIDEN PLAN FOR LEADING THE DEMOCRATIC WORLD TO MEET THE CHALLENGES OF THE 21ST CENTURY, https://joebiden.com/americanleadership [https://perma.cc/TNT7-TMQ8]; *see* Annie Karni & Eric Schmitt, *Biden Takes Two Paths to Wind Down Iraq and Afghan Wars*, N.Y. TIMES (Aug. 25, 2021), https://www.nytimes.com/2021/07/26/us/politics/biden-iraq-afghanistan.html (comparing the Biden administration's withdrawal from Afghanistan to its far more modest changes to the United States' military engagement in Iraq). However, critics claim President Biden's actions stop short of winding down the post-9/11 security apparatus, which has come to define the War on Terror. *See* Samuel Moyn, *Biden Pulled Troops out of Afghanistan. He Didn't End the 'Forever War.'*, WASH. POST (Aug. 17, 2021, 1:27 PM), https://www.washingtonpost.com/outlook/2021/08/17/afghanistan-troop-withdrawal-war-on-terror (arguing that by withdrawing forces from Afghanistan but not renouncing using military force there, President Biden "merely completed the job started by President George W. Bush and his successors: converting the war on terrorism from a conventional military venture to a global operation conducted by such methods as drone strikes, Special Operations raids and standoff missiles"); Max Burns, *Forever Wars Won't End if the Surveillance State's Still Here*, DAILY BEAST (Sept. 4, 2021, 3:50 AM), https://www.thedailybeast.com/forever-wars-wont-end-if-the-surveillance-states-still-here?ref=scroll (emphasizing that winding down the USA Patriot Act's remaining surveillance provisions must be a priority for the Biden administration).

13. *See* Setty, *supra* note 11, at 88 (arguing that reliance on leaked information to trigger accountability is grounds for reconsidering the extreme secrecy under which the government administers intelligence activities); Jameel Jaffer, *What We Owe Whistleblowers*, KNIGHT 1ST AMEND. INST. COLUM. U. (Sept. 9, 2021), https://knightcolumbia.org/content/what-we-owe-whistleblowers [https://perma.cc/G5XY-727E] (detailing the role of whistleblowers in the debate over post-9/11 national security programs, including interrogation, surveillance, and so-called "targeted killings").

14. 965 F.3d 1015 (9th Cir. 2020), *cert. granted*, No. 20-828, 2021 WL 2301971 (U.S. June 7, 2021).

15. *Id.* at 1024; *see infra* notes 138–39 and accompanying text.

information about the surveillance program, it nonetheless argued that the state secrets privilege protected certain information about the program.[16]

The Ninth Circuit disagreed with the FBI, holding that the Foreign Intelligence Surveillance Act of 1978[17] (FISA) displaces the state secrets privilege in electronic surveillance cases.[18] The Ninth Circuit further found that, contrary to the government's contention, courts must use FISA's *in camera*, *ex parte* procedures when an aggrieved person affirmatively challenges the legality of electronic surveillance or its use in litigation in any civil case, whether the challenge is under FISA itself, the Constitution, or any other federal law.[19]

Fazaga provided important support for plaintiffs challenging the lawfulness of the National Security Agency (NSA) surveillance programs that concerned the CJEU in *Schrems II*. However, the Fourth Circuit's rejection of the same FISA preemption in *Wikimedia* indicates that judicial redress may remain elusive.[20] The Supreme Court's grant of the writ of certiorari in two state secrets cases—*Fazaga* and *United*

16. *Id.* at 1028.

17. 50 U.S.C. §§ 1801–85.

18. *Fazaga*, 965 F.3d at 1052. In so holding, the *Fazaga* court recalled FISA's origins in a period when intelligence agencies' widespread infringement of privacy and civil liberties was at the fore of public debate. *Id.* at 1046–47; *see infra* Section I.B.1 (discussing in detail the period preceding FISA's enactment).

19. *Fazaga*, 965 F.3d at 1052; *see infra* Section I.B.2 (explaining the contours of these procedures).

20. In September, the Fourth Circuit, in a divided panel opinion, affirmed the district court grant of summary judgment and rejected the *Fazaga* court's preemption holding. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *1, 16 (4th Cir. Sept. 15, 2021); *see infra* notes 211–34 and accompanying text (detailing the Fourth Circuit's decision). In August, the Ninth Circuit affirmed summary judgment for the NSA in *Jewel v. NSA*, in which several plaintiffs allege that their internet communications, phone records, and metadata have been collected, along with those of millions of Americans, as part of the NSA's surveillance programs. Jewel v. NSA, 856 F. App'x 640, 641–42 (9th Cir. 2021); Appellants' Opening Brief at 7, Jewel v. NSA, No. 19-16066 (9th Cir. Oct. 7, 2019). Unlike the Fourth Circuit, the Ninth Circuit affirmed without considering lower court's finding that state secrets privilege barred plaintiffs' claims. *Jewel*, 856 F. App'x at 641–42.

States v. Zubaydah[21]—indicates the Court may choose to clarify the nature and scope of the privilege.[22]

Providing redress for electronic surveillance and other national security programs is vital to repair the harm done to individuals and communities and restore trust in government institutions.[23] Further, as *Schrems II* shows, the availability of individual redress for unlawful surveillance also has serious implications for relationships with key allies such as the European Union.[24] Therefore, the United States has an interest in providing viable pathways to redress for both U.S. and non-U.S. persons.[25]

This Comment argues that FISA's § 1806(f) procedures displace the state secrets privilege in electronic surveillance cases and that these procedures apply even where the government's invocation of the privilege aims to shield evidence relating to whether a particular plaintiff was subject to surveillance, thus making them an "aggrieved person" under FISA.

Part I of this Comment proceeds along two tracks. First, it traces the development and abuse of electronic surveillance, Congress's adoption of FISA as a mechanism for accountability, and the renewed debate over electronic surveillance and individual redress in the post-9/11 era. Second, it explores the development of the modern state secrets privilege and its role in post-9/11 national security litigation, particularly in challenges to electronic surveillance programs. Part II analyzes FISA's text and legislative history pertaining to challenges of unlawful surveillance, as well as related national security

---

21. 965 F.3d 775 (9th Cir. 2020), *cert. granted*, No. 20-827, 2021 WL 1602639 (U.S. Apr. 26, 2021). Zayn al-Abidin Muhammad Husayn, also known as Abu Zubaydah, is a Guantanamo Bay detainee and the first prisoner held in CIA custody who was subjected to the CIA's "enhanced interrogation techniques" that are seen by many as torture. *See infra* note 112 (describing in detail the CIA program). Abu Zubaydah is seeking to subpoena two former CIA contractors as part of legal proceedings in Poland relating to the CIA program. Husayn v. Mitchell, 938 F.3d 1123, 1126 (9th Cir. 2019).

22. *See infra* note 246 and accompanying text (exploring the potential avenues for Supreme Court review).

23. *See* S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTEL. ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 292 (1976) [hereinafter CHURCH COMMITTEE REPORT] ("Lawlessness by Government breeds corrosive cynicism among the people and erodes the trust upon which government depends.").

24. *See infra* Section III.A.

25. In recent years, the U.S. has made progress extending some protection to non-U.S. persons. *See infra* notes 81–82 and accompanying text (detailing PPD-28).

jurisprudence, to argue that, although the state secrets privilege has "constitutional overtones,"[26] it is an evidentiary privilege at its core. This Part then examines the split between the Fourth and Ninth Circuits over FISA preemption and argues that courts in electronic surveillance cases must follow FISA's *in camera*, *ex parte* procedures prior to accepting the government's invocation of the state secrets privilege to preclude plaintiffs from obtaining evidence confirming or denying that they were subject to surveillance. Part II then emphasizes the importance of mechanisms for judicial redress in electronic surveillance cases in aligning the United States and European Union on data privacy in the wake of *Schrems II*. This Comment concludes that FISA's procedures offer an important opportunity for redress, despite remaining secretive and deferential to the government.

I. BACKGROUND: SURVEILLANCE, SECRECY, AND REDRESS

Secrecy is essential to many national security activities;[27] however, it also comes with considerable costs—namely, weakened external oversight and a lack of public understanding of and debate over government activities carried out on the public's behalf.[28] Despite these challenges, both Congress and the judiciary play important roles in preventing abuse, providing oversight, and establishing a framework for redress.[29] However, individual plaintiffs challenging the lawfulness of an electronic surveillance program face myriad obstacles.[30] One of

26. United States v. Reynolds, 345 U.S. 1, 6 (1953).

27. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 319 (1972) ("Secrecy is the essential ingredient in intelligence gathering . . . .").

28. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 103 (2004) ("Secrecy, while necessary, can also harm oversight."); PUB. INTEREST DECLASSIFICATION BD., TRANSFORMING THE SECURITY CLASSIFICATION SYSTEM 6 (2012), http://www.archives.gov/declassification/pidb/recommendations/transforming-classification.pdf [https://perma.cc/W22F-JHAT] ("At its most benign, secrecy impedes informed government decisions and an informed public; at worst, it enables corruption and malfeasance.").

29. *See* Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2254 (2016) (emphasizing the need for both "vigorous and effective" national security programs and useful constraints on those programs). *See generally* Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931 (2007) (exploring legislative and judicial collaboration in overseeing the executive branch).

30. *See generally* Vladeck, *supra* note 10, at 1037 (examining structural and procedural obstacles to civil suits against the government arising out of national security programs).

the most significant obstacles is the state secrets privilege, which prevents information from public disclosure to preserve national security.[31]

Section I.A discusses the development and abuse of electronic surveillance by intelligence agencies in the post-World War II era, the creation of FISA as a check on excessive executive power and secrecy in electronic surveillance, and the evolution of electronic surveillance in the post-9/11 era. Section I.B examines the state secrets privilege and the development of the FISA preemption argument in surveillance litigation arising out of post-9/11 counterterrorism programs.

A. Development and Abuse of Electronic Surveillance

Electronic surveillance is a key component of intelligence agencies' activities, particularly those of the NSA.[32] However, as with other forms of new technology, the implementation of electronic surveillance has historically outpaced efforts to regulate it, leading to concerns of abuse and public blowback.[33]

---

31. *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1266–69, 1285–86 (2007) (noting criticism of the state secrets privilege as a barrier to accountability because a successful claim of privilege results in either the removal of the privileged information from litigation or, in some circumstances, the dismissal of the entire action).

32. *See* Glenn S. Gerstell, Nat'l Sec. Agency & Cent. Sec. Serv. Gen. Couns., Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act, (Sept. 14, 2017), https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?ProtalId=70&ModuleId=9757&Article=1619167 [https://perma.cc/P7BK-9RG9] (referring to the Section 702 program—discussed at length later in this section—as "one of NSA's most important intelligence surveillance authorities," which "provides tremendous value in the nation's fight against foreign terrorists"); Press Release, Nat'l Sec. Agency, The National Security Agency: Missions, Authorities, Oversight and Partnerships (Aug. 9, 2013), [https://perma.cc/9EV3-EYN9]; *see* Priv. & Civ. Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 2 (2014) [hereinafter PCLOB Section 702 Report], https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf [https://perma.cc/C7J9-S3CH] (finding that the information collected under the NSA's section 702 programs "has been valuable and effective in protecting the nation's security and producing useful foreign intelligence").

33. *See infra* Sections I.B.1, I.B.3 (detailing such periods of upheaval in the 1970s and the early twenty-first century).

1. The origins of surveillance

The United States began wiretapping shortly after the invention of electronic communication.[34] However, attempts to regulate wiretapping were slow to emerge, especially at the federal level; until FISA's enactment in 1978, there was practically no judicial or legislative oversight of wiretapping or other forms of electronic surveillance as part of national security programs.[35]

While the United States engaged in surveillance throughout the late nineteenth and early twentieth centuries, it was only in 1940, just before the United States entered World War II, that electronic surveillance became integral to national security and intelligence activities.[36] As part of the United States' efforts to combat "subversive activities," President Roosevelt authorized the domestic use of surveillance in the name of national security.[37] However, coming out of World War II, U.S. intelligence agencies "systematically broke the law," with operations moving beyond targeting traditional foreign threats to targeting domestic groups including the civil rights and anti-war movements.[38] Intelligence agencies relied on extreme measures in targeting these groups, including the interception and reading of first-

---

34. *See* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3:2 (3d ed. 2019) (providing history of the development of electronic surveillance as early as the Civil War).

35. *Id.* § 3:1. The Supreme Court's 1928 decision in *Olmstead v. United States* placed most electronic surveillance outside the scope of the Fourth Amendment. 277 U.S. 438, 464 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); *see* KRIS & WILSON, *supra* note 34, § 3:2 ("By placing most electronic surveillance outside the scope of the Fourth Amendment, that decision ceded nearly all control of wiretapping to Congress and the executive branch."). It was only in 1967 that the Court overruled *Olmstead*, bringing surveillance under the Fourth Amendment framework. *See Katz*, 389 U.S. at 353 (holding that surveillance of an individual's phone call in a telephone booth constituted a search under the Fourth Amendment). While there is debate about the tensions between the FISA system and the Fourth Amendment, these issues are beyond the scope of this Comment.

36. *See* CHURCH COMMITTEE REPORT, *supra* note 23, at 36–37 (discussing the authorization of wiretapping against "persons suspected of subversive activities against the United States").

37. *Id.* at 25–28.

38. KRIS & WILSON, *supra* note 34, § 2:2; CHURCH COMMITTEE REPORT, *supra* note 23, at 71–74; *see id.* at 137–38 (summarizing its findings that domestic intelligence activities violated both statutory and constitutional rights, either because these rights were either not considered or because they were "intentionally disregarded in the believe that because the programs served the 'national security' the law did not apply").

class mail and telegrams and covert operations to smear public figures.[39]

Electronic surveillance programs formed an important part of these abusive intelligence activities. Between 1945 and 1975, the NSA and its predecessor organizations—operating under the code name "Operation Shamrock"—collaborated with international telegraph companies to obtain copies of most international telegrams leaving the United States.[40] At the time, Shamrock was likely the single largest electronic surveillance operation to affect American citizens.[41]

2. The Church Committee and calls for intelligence reform and accountability

In 1975, in response to the Watergate scandal and other revelations of government abuse,[42] Congress created two committees to investigate intelligence activities.[43] The Church Committee—named after its chair, Senator Frank Church—investigated and reported on abuses by the Central Intelligence Agency (CIA), the NSA, the FBI, and the Internal Revenue Service (IRS).[44] The Church Committee concluded that "intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."[45] The Church Committee noted that previous efforts to limit domestic intelligence activities had proven

---

39. KRIS & WILSON, *supra* note 36, § 2:2.

40. CHURCH COMMITTEE REPORT, *supra* note 23, at 104.

41. KRIS & WILSON, *supra* note 34, § 2.3.

42. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, U.S. SENATE, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm [https://perma.cc/KS9B-FT49].

43. *See generally* CHURCH COMMITTEE REPORT, *supra* note 23, at 373 (explaining how the Watergate investigation exposed the need for Congress to review intelligence agencies' structure and programs).

44. *Id.* While this Comment focuses on NSA activities, several other programs have garnered significant attention. In particular, the Church Committee revealed that the CIA had engaged in a wide range of abusive actions abroad, including plots to assassinate foreign leaders. *Id.* Meanwhile, at home, the FBI's Counterintelligence Program (COINTELPRO) targeted suspected communists or other "subversives," including members of the civil rights movement, the anti-Vietnam War movement, as well as state, local, and federal officials. *Id.* at 10, 22. In likely the most infamous instance, the FBI mailed a note with a tape recording to civil rights leader Dr. Martin Luther King, Jr., which Dr. King and his advisors interpreted as a threat to ruin Dr. King's marriage unless he committed suicide. *Id.* at 11.

45. *Id.* at 289.

ineffectual, largely due to excessive executive power and secrecy.[46] The Church Committee emphasized that these past efforts and patterns of abuse underscored the need for Congress and the judiciary to provide more robust oversight.[47]

The Church Committee recommended judicial review of intelligence activity before or after the fact, as well as the enactment of "a comprehensive civil remedy," imbuing the courts with jurisdiction over "legitimate complaints by citizens injured by unconstitutional or illegal activities of intelligence agencies."[48] A civil remedy, the Church Committee reasoned, would deter improper intelligence activity and afford effective redress to people who suffered harm resulting from unlawful intelligence activity.[49] Additionally, the Church Committee recommended criminal penalties for cases of gross abuse and the requirement of judicial warrants before intelligence agencies could use certain intrusive techniques.[50]

Addressing the NSA, the Church Committee recommended the creation of a statutory framework governing NSA's activities with several primary goals in mind: limiting NSA to the collection of foreign intelligence from foreign communications; eliminating or minimizing the interception, selection, and monitoring of Americans' communications as part of foreign intelligence collection; requiring government entities to obtain a warrant prior to collecting communications to, from, or about U.S. persons; and curtailing the NSA's relationships with commercial carriers.[51]

The Church Committee emphasized that these recommendations "should be embodied in a comprehensive legislative charter defining and controlling the domestic security activities of the Federal Government."[52] In 1978, as part of a period of legislative activism

---

46. *See id.* at 292 (acknowledging the longstanding view in Congress and the courts that control of intelligence activities was exclusive to the executive branch and emphasizing that executive power viewed as inherent in the Presidency "contained the seeds of abuse").

47. *Id.* at 289.

48. *Id.* at 293–94.

49. *Id.* at 336.

50. *Id.* at 294.

51. *Id.* at 309–10. As the Church Committee noted, several of its recommendations specifically aimed to prevent the NSA from reestablishing its "watch list[]" and Shamrock programs. *Id.* at 310.

52. *Id.* at 293.

arising out of these same executive branch abuses, Congress enacted FISA, adopting many of the Church Committee's recommendations.[53]

3. FISA procedures

Through FISA, Congress established comprehensive legislation for electronic surveillance and imposed more stringent requirements for conducting such surveillance. Under FISA, the government must obtain a warrant from a specialized court—the Foreign Intelligence Surveillance Court (FISC)—to acquire communications to or from people in the United States.[54] Congress also unambiguously stipulated that it intended FISA to be the "exclusive means" by which the government could lawfully conduct electronic surveillance.[55]

Additionally, FISA adopted the Church Committee's recommendation for an expanded civil remedy scheme.[56] Section 110 of FISA grants a private right of action to individuals harmed by government violations of FISA's procedures. In relevant part, § 110 provides:

> [a]n aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation. . . .[57]

---

53. *Compare* 50 U.S.C. §§ 1801–13 (codifying the Church Committee's recommended restraints on electronic surveillance) *with* CHURCH COMMITTEE REPORT, *supra* note 23, at 296–339 (encouraging Congress to pass comprehensive legislation to control the federal government's domestic surveillance activities, including ninety-six specific recommendations). During this same period, Congress enacted the Privacy Act of 1974, amended the Freedom of Information Act (FOIA), established intelligence oversight committees in both the House and Senate, and passed the War Powers Resolution. *See* Kathryn Olmstead, *Watergate Led to Sweeping Reforms. Here's What We'll Need After Trump*, WASH. POST (Nov. 15, 2019), https://www.washingtonpost.com/outlook/2019/11/15/watergate-led-sweeping-reforms-heres-what-well-need-after-trump.

54. *Id.*

55. 50 U.S.C. § 1812; *see also* 18 U.S.C. § 2511(2)(f). FISA's exclusivity provision was derived from another of the Church Committee's recommendations. *See* CHURCH COMMITTEE REPORT, *supra* note 23, at 297 (recommending that statutes implementing the Church Committee's findings "provide the exclusive legal authority for federal domestic security activities").

56. 50 U.S.C. § 1810.

57. *Id.*

FISA also empowers courts to determine the lawfulness of electronic surveillance through its *in camera*, *ex parte* procedures.[58] According to these procedures, federal district courts shall, notwithstanding any other law, conduct an *in camera*, *ex parte* review to determine the lawfulness of electronic surveillance when the issue arises in a case and the Attorney General files an affidavit that disclosure or an adversary hearing would harm national security.[59] Such a circumstance could arise in three situations: (1) in a proceeding when the government gives notice that it plans to use information obtained or derived from electronic surveillance against a person who has been subjected to the surveillance; (2) when such a person moves to suppress the evidence obtained or derived from electronic surveillance; or (3) when such a person otherwise moves to discover or obtain information derived from electronic surveillance under FISA.[60] Only in extraordinary circumstances—when necessary to determine the lawfulness of the surveillance—may a court disclose portions of the material at issue to the aggrieved person.[61]

FISA's provisions established guidelines for electronic surveillance in the modern era by comprehensively regulating intelligence activities. Decades later, the 9/11 attacks and wide-scale technological development set in motion electronic surveillance programs that would threaten public faith in the U.S. intelligence community.[62]

4. Modern surveillance and calls for redress

In response to the 9/11 attacks, the U.S. government greatly expanded its surveillance operations, including by authorizing electronic surveillance within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.[63] The Bush White House authorized the NSA to

58. *Id.* § 1806(f).

59. *Id.*

60. *See* ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 462 (D.C. Cir. 1991) (citing 50 U.S.C. § 1806(f)).

61. *See* 50 U.S.C. § 1806(f) (noting that any disclosure must be subject to "appropriate security procedures and protective orders").

62. In particular, the birth of the internet and modern digital technology has enabled government agencies to both collect quantities of information not previously feasible, as well as types of information not previously available absent prohibitive cost. David D. Cole, *After Snowden: Regulating Technology-Aided Surveillance*, 44 CAP. U. L. REV. 677, 680–81 (2016).

63. *See* Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, BRENNAN CTR. FOR JUST. 25 (2015), https://www.brennancenter.org/sites/default/

collect: (1) the contents of certain international communications, a program that was later referred to as the Terrorist Surveillance Program ("TSP");[64] and (2) telephony and Internet non-content information (referred to as "metadata") in bulk, subject to various conditions.[65] After the press revealed the existence of the TSP in 2005, the government obtained FISC authorization to conduct the TSP's collection programs under the FISA legal framework.[66] Congress then developed its own statutory framework authorizing and governing these collection programs, and it has continued to reauthorize many of these programs to keep pace with rapidly changing technology.[67]

Congress passed the FISA Amendments Act of 2008,[68] which "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA, for targets reasonably believed to be abroad."[69] Section 702 authorizes surveillance conducted within the United States but only when targeting non-U.S. persons "reasonably believed to be located outside the United States."[70] Although section 702 does not authorize

---

files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf ("[I]n the immediate aftermath of 9/11 . . . the Bush administration began intercepting communications to and from Americans without seeking any type of judicial approval."); *see also* OFFS. OF INSPECTORS GEN. OF THE DEP'T OF JUSTICE ET AL., REP. NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 1, 1, 12–13 (July 10, 2009), https://irp.fas.org/eprint/psp.pdf [https://perma.cc/7JWS-CKGS] (discussing legal analysis conducted by the DOJ Office of Legal Counsel Deputy Assistant Attorney General, John Yoo, which found that post-9/11 surveillance operations were "reasonable" and thus did not require a judicial warrant).

64. The TSP authorized the NSA to intercept communications where there was a reasonable basis to conclude that one party to the communication was a member of al-Qaeda or a related terrorist organization. OFFS. OF INSPECTOR GEN. OF THE DEP'T OF DEF. ET AL., *supra* note 63, at 1.

65. PCLOB SECTION 702 REPORT, *supra* note 32, at 16. The perception that the 9/11 attacks resulted from intelligence failures precipitated the subsequent effort to enhance intelligence programs and led to the loosening of legal and policy constraints on intelligence gathering. Setty, *supra* note 10, at 72.

66. CHARLIE SAVAGE, POWER WARS: THE RELENTLESS RISE OF PRESIDENTIAL AUTHORITY AND SECRECY 196–202 (rev. ed. 2017); PCLOB SECTION 702 REPORT, *supra* note 32, at 5.

67. PCLOB SECTION 702 REPORT, *supra* note 32, at 5; KRIS & WILSON, *supra* note 34, § 3:9.

68. Pub. L. No. 110-261, 122 Stat. 2436.

69. KRIS & WILSON, *supra* note 34, § 9:13. *See generally* 50 U.S.C. § 1881a (requiring certain procedures for targeting non-U.S. persons abroad).

70. 50 U.S.C. § 1881a. Under FISA, "U.S. persons" includes U.S. citizens, U.S. permanent residents, unincorporated associations substantially composed of U.S.

surveillance targeting U.S. persons, "communications of or concerning U.S. persons may be acquired in a variety of ways."[71] Unlike traditional FISA, section 702 does not require intelligence agencies to obtain a warrant or prior approval from the FISC before surveilling any particular individual; rather, the FISC authorizes gathering of particular types of foreign intelligence, as well as the procedures governing targeting and handling of that intelligence.[72]

The government has acknowledged that it conducts section 702 surveillance through two programs, including Upstream.[73] Pursuant to the Upstream program, the NSA intercepts communications transiting internet "backbone" circuits and scans those communications for "selectors" associated with targeted individuals.[74]

In June 2013, former NSA contractor Edward Snowden stole and publicly disclosed a huge trove of classified documents, including many detailing the scope and nature of NSA surveillance on foreign and U.S. persons.[75] While the U.S. government maintains that Snowden's actions caused "grave" damage to U.S. intelligence capabilities,[76] the disclosures resulted in a public reckoning over surveillance that continues to this day and led to significant intelligence oversight reform.[77] However, most technical details

---

citizens, and most U.S. corporations. PCLOB SECTION 702 Report, *supra* note 32, at 1 n.2, 106 n.466.

71. PCLOB SECTION 702 REPORT, *supra* note 32, at 6. "Incidental" collection is when a U.S. person communicates with a non-U.S. person targeted by surveillance. *Id.* U.S. person communications may also be subject to "inadvertent" collection due to a mistake or technological issue. *Id.*

72. *Id.* at 89.

73. *Id.* at 7.

74. *Id.* "Backbone" circuits are those used to facilitate internet communications. *Id.* at 36–37. "Selectors" include information such as telephone numbers or email addresses. *Id.* at 7.

75. Setty, *supra* note 11, at 73.

76. *See* Jason Leopold, *Pentagon Report: Scope of Intelligence Compromised by Snowden 'Staggering'*, GUARDIAN (May 22, 2014), https://www.theguardian.com/world/2014/may/22/pentagon-report-snowden-leaks-national-security [https://perma.cc/4XZE-T96M].

77. *See* SAVAGE, *supra* note 66, at 195–200 (identifying the repercussions of the Snowden leaks, which led to "a harsh public spotlight on the FISA Court's role in facilitating" NSA surveillance); Setty, *supra* note 11, at 73–74 (noting that after the Snowden disclosures, the Obama administration and Congress responded by conducting reviews and hearings, and the American public debated the "legality, efficacy and morality" of the NSA's bulk collection and retention of data on U.S. persons). The Privacy and Civil Liberties Oversight Board (PCLOB), established by

remain classified, even with the government's greater effort to provide transparency.[78]

The Snowden disclosures set off similar debates over privacy and surveillance in Europe.[79] The European response to revelations of the NSA's surveillance has also implicated longstanding E.U.-U.S. data-sharing agreements, including the E.U.-U.S. Privacy Shield.[80] The United States has implemented some reforms pertaining to non-U.S. persons. In 2014, then President Barack Obama introduced Presidential Policy Directive 28 ("PPD-28"), which required the intelligence community to develop and implement greater privacy

---

Congress in 2004, played an active role in assessing both the efficacy of these programs, as well as their intrusions into civil liberties. *See id.* at 101 (praising the PCLOB's broad mandate and relatively high level of independence from the executive branch); *see also* PRIV. & CIV. LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 16 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/DW47-ZGBT] (recommending the government end its section 215 bulk telephone records program); PCLOB SECTION 702 REPORT, *supra* note 32, at 12–13 (recommending a number of revisions to the section 702 program in order to better balance national security, privacy, and civil liberties). In 2018, Congress reauthorized the FISA Amendments Act for another five years but added new restrictions on the querying of collected data. KRIS & WILSON, *supra* note 34, § 3:9. Among other requirements, the Act dictates that the Attorney General and Director of National Intelligence (DNI) must adopt procedures "consistent with the requirements of the [F]ourth [A]mendment" for querying information derived from section 702 surveillance; these procedures are subject to FISC review. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118 § 101(f)(1), 132 Stat. 3, 4 (2018).

78. Wikimedia Found. v. NSA, 857 F.3d 193, 202 (4th Cir. 2017) (citing Jewel v. NSA, 810 F.3d 622, 627 (9th Cir. 2015)). Two particularly notable avenues for transparency have been the declassification of certain FISC opinions, as well as the ODNI's creation of the *IC on the Record* blog and database. *See* IC ON THE RECORD, https://icontherecord.tumblr.com/ [https://perma.cc/K3TN-GBAA].

79. *See* Alan Butler & Fanny Hidvegi, *From Snowden to* Schrems*: How the Surveillance Debate has Impacted US-EU Relations and the Future of International Data Protection*, 17 WHITEHEAD J. DIPL. & INT'L REL. 55, 55 (2015–2016) (noting how the Snowden revelations "fundamentally altered" E.U.-U.S. negotiations over data protection).

80. Privacy Shield, created in 2016, replaced a similar E.U.-U.S. data transfer mechanism, the Safe Harbor Agreement of 2000, which the CJEU struck down in 2015. RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF11613, U.S.-EU PRIVACY SHIELD (2021). Privacy Shield provided over 5,000 companies with a mechanism to transfer E.U. citizens' personal data to the United States in compliance with E.U. data protection laws. *Id.*

protections, including by extending certain protections to non-U.S. persons.[81] However, PPD-28 did not create a judicially enforceable right of action, and as NSA surveillance cases have progressed through U.S. courts, international privacy standards have put pressure on the United States to further reform its surveillance framework, including by reaffirming that there are viable pathways to redress.[82]

In 2013, privacy activist Max Schrems filed a complaint to prohibit Facebook Ireland from transferring his personal data to the United States, claiming that U.S. law did not adequately protect his personal data held in its territory from U.S. government surveillance when it was transported or hosted within U.S. territory.[83] In *Schrems II*, the CJEU invalidated the E.U.-U.S. Privacy Shield, in part, because parties injured by surveillance lacked a private right of action in U.S. courts.[84] While the CJEU emphasized some of the statutory obstacles to redress for unlawful surveillance in U.S. courts, it neglected to address an important judicially created obstacle that has long stymied efforts for redress in national security matters—the state secrets privilege.[85]

B. The State Secrets Privilege

The state secrets privilege prevents the disclosure of certain evidence or causes the dismissal of a case entirely because such disclosure would harm national security.[86] While Congress and the judiciary have both recognized the executive branch's need to maintain some level of secrecy, debate remains over whether the state secrets privilege is

---

81. Press Release, Off. of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/CVW8-Q2J8].

82. *See* Henry Farrell & Abraham L. Newman, Schrems II *Offers an Opportunity—If the U.S. Wants to Take It*, LAWFARE (July 28, 2020, 9:01 AM), https://www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it [https://perma.cc/MLW9-8XX3] (detailing why the United States should engage positively with European courts' demands for privacy protection).

83. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 50–52 (July 16, 2020).

84. *Id.* at ¶¶ 178–85.

85. *See* Vladeck, *supra* note 10, at 1066–67 (noting that the privilege has figured prominently in post-9/11 civil litigation).

86. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc) (citing Totten v. United States, 92 U.S. 105, 107 (1876)) (recognizing the Supreme Court's precedent of dismissing cases that risk disclosure of state secrets in exceptional circumstances).

constitutionally based or merely a federal common law evidentiary rule.[87] Further, debate remains over the amount of deference owed to the government when it invokes the privilege at the expense of a plaintiff claiming serious harm arising out of government action.[88]

1. The modern state secrets privilege

The modern state secrets privilege crystallized in post-World War II litigation arose out of the ensuing expansion of military activity, both domestically and internationally.[89] The state secrets privilege is comprised of two distinct doctrines, which the Supreme Court established in *Totten v. United States*[90] and *United States v. Reynolds*.[91] The *Totten* bar completely prevents claim adjudication "'where the very subject matter of the action' is 'a matter of state secret.'"[92] Meanwhile, the *Reynolds* privilege, which courts have generally interpreted as rooted in federal common law, allows the government to prevent the disclosure of certain evidence if such disclosure would harm national security.[93]

In *Reynolds*, widows of three Air Force contractors brought a wrongful death suit against the government after their husbands died

87. *See infra* Section I.B.2.

88. *Jeppesen*, 614 F.3d at 1073 (emphasizing "the difficult balance the state secrets doctrine strikes between fundamental principles of our liberty, including justice, transparency, accountability and national security").

89. Chesney, *supra* note 31, at 1281; *see* James Zagel, *The State Secrets Privilege*, 50 MINN. L. REV. 875, 878 (1966) (noting that after World War II, the clear line between wartime and peacetime had broken down and large segments of industry were constantly occupied with national defense).

90. 92 U.S. 105 (1876).

91. 345 U.S. 1 (1953).

92. *Jeppesen*, 614 F.3d at 1077–78 (quoting *Reynolds*, 345 U.S. at 11 n.26).

93. *See, e.g.*, Gen. Dynamics Corp. v. United States, 563 U.S. 478, 485 (2011) ("*Reynolds* was about the admission of evidence. It decided a purely evidentiary dispute by applying evidentiary rules: The privileged information is excluded and the trial goes on without it."); *Jeppesen*, 614 F.3d at 1077 (referring to the state secrets as an evidentiary privilege); *see also* Frost, *supra* note 29, at 1954 (noting that "litigants and courts addressing the state secrets privilege have viewed it as an evidentiary restriction, and not as the executive's attempt to carve out a set of cases from the jurisdiction conferred on the courts by Congress"). Nonetheless, the government and a number of legal authorities continue to claim that the privilege is an outgrowth of the separation of powers and executive privilege. *See, e.g.*, Letter from Michael B. Mukasey, U.S. Att'y Gen., to Sen. Patrick J. Leahy, Chairman of the Senate Comm. on the Judiciary, (Mar. 31, 2008), https://fas.org/sgp/jud/statesec/ag033108.pdf [https://perma.cc/V9FW-M4JB] (claiming that the state secrets privilege is within the executive branch's authority under Article II to control access to national security information).

in a plane crash while testing secret equipment.[94] In both the district court and the Third Circuit, the government initially sought to suppress the crash report on other grounds but eventually claimed it would harm national security.[95] However, both courts rejected this argument, ordering the government to turn over the documents so that the court could determine whether they were privileged.[96]

On appeal, the Supreme Court acknowledged the executive power to withhold documents, which the Court noted has "constitutional overtones," but found that it was unnecessary to address that issue because a narrower ground for decision was available.[97] According to the Court, the Secretary of the Air Force, in lodging his formal claim of privilege, attempted to invoke the privilege against revealing military secrets, "a privilege which is well established in the law of evidence."[98]

Judge Vinson, writing for the Court, detailed a number of procedural requirements for invoking the privilege and then proceeded to lay out the standards by which courts should probe the invocation of the privilege.[99] In doing so, Judge Vinson sought to reconcile the tension between ensuring effective judicial control of evidence and preserving the secrecy of legitimately sensitive information.[100] Therefore, according to Judge Vinson, courts should generally weigh the plaintiff's showing of necessity against the invocation of the privilege.[101] However, Judge Vinson stopped short of endorsing mandatory *in camera*, *ex parte* procedures, and instead found that there may be scenarios in which the court may find disclosure presents a reasonable danger to national security without examining the documents themselves.[102] Turning to the facts of the case, Judge Vinson found that because the widows had reasonable opportunity to interview surviving crew members, the necessity of producing the crash

94. *Reynolds*, 345 U.S. at 2–3.
95. *Id.* at 3–4.
96. *Id.* at 5.
97. *Id.* at 6.
98. *Id.* at 6–7.
99. *Id.* at 7–11.
100. *See id.* at 9–10 (emphasizing that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers," but that the Court—where possible—should avoid "jeopardiz[ing] the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers").
101. *Id.* at 11.
102. *Id.* at 9–10.

report did not overcome the government's invocation of the privilege.[103] In so finding, the Court declined to examine the report to scrutinize the propriety of the invocation.

Reynolds remains controversial, both for its legal analysis and as a cautionary tale of government secrecy claims. After the government released the declassified report decades later, it contained significant evidence of negligence but no discernible sensitive national security information, "transforming the landmark case, at least in the eyes of its critics, into a symbol of abuse of secrecy powers."[104]

Nonetheless, the state secrets doctrine set forth by the *Reynolds* court has lived on. In the decades since *Reynolds*, courts have used a three-step analysis to evaluate assertions of the *Reynolds* privilege. First, the court must "ascertain that the procedural requirements for invoking the state secrets privilege have been satisfied."[105] These procedural requirements include the presence of a sufficiently detailed formal claim by the appropriate head of the department.[106] Second, the court must independently determine whether the information is privileged.[107] The court will sustain a claim of privilege when it finds

---

103. *Id.* at 11.

104. SAVAGE, *supra* note 66, at 738 n.2. In 2003, several of the widows' daughters, along with one of the surviving widows, sought a writ of error in *coram nobis* at the Supreme Court, arguing that the government had perpetrated a fraud on the court. *See generally* LOUIS FISHER, IN THE NAME OF NATIONAL SECURITY: UNCHECKED PRESIDENTIAL POWER AND THE REYNOLDS CASE (2006) (tracing the history of the *Reynolds* litigation); BARRY SIEGEL, CLAIM OF PRIVILEGE: A MYSTERIOUS PLANE CRASH, A LANDMARK SUPREME COURT CASE, AND THE RISE OF STATE SECRETS (2008) (same). In their petition, the plaintiffs drew parallels to several cases in which courts had issued writs of error *coram nobis* to overturn the convictions of Japanese-American individuals interned during World War II as a result of deliberately false and misleading government submissions of military necessity. *See* SIEGEL, *supra*, at 261–308 (chronicling the unsuccessful second wave of litigation).

105. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc) (quoting Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1202 (9th Cir. 2007) (quoting El-Masri v. United States, 479 F.3d 296, 304 (4th Cir. 2007))).

106. *Id.* at 1080. Such a claim can be asserted at any time, even preemptively. *Id.* The government need not even be an originally named party to a case to invoke the privilege. TODD GARVEY & EDWARD C. LIU, CONG. RSCH. SERV., R41741, THE STATE SECRETS PRIVILEGE: PREVENTING THE DISCLOSURE OF SENSITIVE NATIONAL SECURITY INFORMATION DURING CIVIL LITIGATION 3 (2011) (noting that the government can assert the state secrets privilege when it is not a party if "litigation could . . . lead to the disclosure of secret evidence that would threaten national security").

107. *Jeppesen*, 614 F.3d at 1080. While courts defer to the executive branch on national security matters, they have emphasized the serious obligation of courts to review state secrets privilege claims "with a very careful, indeed a skeptical, eye, and

that, under the totality of the circumstances, there is a reasonable danger that compulsion of the evidence will disclose state secrets.[108] Third, the court must then decide how the case should proceed in light of the successful privilege claim.[109] The court may either attempt to disentangle privileged information from disclosable information or, if no such disentanglement is possible, the court may dismiss the case entirely.[110]

The *Reynolds* privilege will justify dismissal of the action in three circumstances: (1) if "the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence"; (2) if "the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim"; or (3) if the privileged evidence is "inseparable from nonprivileged information that will be necessary to the claims or defenses" such that "litigating the case to a judgement on the merits would present an unacceptable risk of disclosing state secrets."[111]

---

not to accept at face value the government's claim or justification of privilege." *Al-Haramain*, 507 F.3d at 1203 ("Simply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege.").

108. *Jeppesen*, 614 F.3d at 1081 (quoting *Reynolds*, 345 U.S. at 10). The Court in *Reynolds* emphasized that when a court finds that such a danger exists, it "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." *Reynolds*, 345 U.S. at 10.

109. *Jeppesen*, 614 F.3d at 1080.

110. *Id.* at 1082–83.

111. *Id.* at 1083 (quoting Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998)). While *Jeppesen* did not define what constitutes a "valid defense," the Ninth Circuit later adopted the D.C. Circuit's definition and reasoning. Fazaga v. FBI, 965 F.3d 1015, 1067 (9th Cir. 2020), *cert. granted*, No. 20-828, 2021 WL 2301971 (U.S. June 7, 2021). In *In re Sealed Case*, the D.C. Circuit explained that, to be a "valid defense" that would require judgment for the defendant, there must be a meritorious, not merely a plausible, defense. 494 F.3d 139, 149–51 (D.C. Cir. 2007) (explaining "allowing the mere prospect of a privileged defense to thwart" a lawsuit would inappropriately preclude review of constitutional claims and conflict with the Supreme Court's rule against broadly interpreting evidentiary privileges). Therefore, the D.C. Circuit held that a court "may properly dismiss a complaint because of the unavailability of a defense" only after finding in an "appropriately tailored *in camera* review of the privileged record" that the "truthful state of affairs would deny the defendant a valid defense" and influence the case's outcome. *Id.* at 151 (internal citation omitted).

2. Use of the state secrets privilege as a barrier to redress

In the post-9/11 era, the government has often invoked the state secrets privilege in two types of cases—those arising out of the CIA's Rendition, Detention, and Interrogation Program[112] and those arising from NSA surveillance.[113] In both situations, plaintiffs have sought redress for alleged abuses but have failed to pierce the veil of state secrecy.[114]

---

112. *See, e.g.*, *Jeppesen*, 614 F.3d 1070 (government intervening in a suit against a company alleged to have participated in the CIA's extraordinary rendition program); El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007) (government intervening in a suit against the former CIA director arising out of the CIA program). The CIA conducted the Detention and Interrogation Program between 2001 and 2009. S. REP. NO. 113-288, at 8 (2014). During that time, the CIA, authorized by the White House and Department of Justice, used so-called "enhanced interrogation techniques" on detainees captured after 9/11. *Id.* at xi. The CIA subjected at least 39 of the 119 detainees in its custody to these techniques, including Abu Zubaydah, whose case the Supreme Court will hear in October. *Id.* at xii, xxi. According to a number of U.S. government officials, members of Congress, U.N. experts, human rights groups, and at least one federal circuit court, these techniques constitute torture or cruel, inhumane, or degrading treatment, in violation of U.S. and international law. *See* Husayn v. Mitchell, 938 F.3d 1123, 1127 (9th Cir. 2019) ("To use colloquial terms, . . . Abu Zubaydah was tortured."); Shane Harris & Ellen Nakashima, *Avril Haines, Biden's nominee for DNI, Faces Questions on China, Domestic Extremism*, WASH. POST (Jan. 19, 2021), https://www.washingtonpost.com/national-security/biden-haines-director-national-intelligence/2021/01/19/8ed875a2-5a7f-11eb-a976-bad6431e03e2_story.html (quoting Avril Haines's remarks at her confirmation hearing, in which she noted: "I believe that waterboarding is, in fact, torture—constitutes torture under the law . . . . And I believe all of those techniques that involve cruel, inhuman, degrading treatment are unlawful"); Josh Gerstein, *Obama: 'We Tortured Some Folks'*, POLITICO (Aug. 1, 2014), https://www.politico.com/story/2014/08/john-brennan-torture-cia-109654 (quoting then President Obama as saying, "When we engaged in some of these enhanced interrogation techniques, techniques that I believe and I think any fair-minded person would believe were torture, we crossed a line. And that needs to be understood and accepted").

113. *See, e.g.*, Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190 (9th Cir. 2007) (affirmative challenge to the TSP); Jewel v. NSA, 965 F. Supp. 2d 1090 (N.D. Cal. 2013) (affirmative challenge to the NSA's Upstream surveillance program); Wikimedia Found. v. NSA, 427 F. Supp. 3d 582 (D. Md. 2019) (same). Other notable recent suits in which the state secrets privilege has arisen include a U.S. citizen's suit challenging his alleged placement on a "kill list" by U.S. authorities in Syria, and a lawsuit brought by relatives of the victims of 9/11 accusing Saudi Arabia of being complicit in the attacks. *See* Kareem v. Haspel, 986 F.3d 859, 861–65 (D.C. Cir. 2021); *In re Terrorist Attacks on September 11, 2001*, 2021 WL 839455, at *1, *9–14 (S.D.N.Y. Mar. 4, 2021).

114. In some cases, the court dismissed the plaintiffs' suits after finding that the very subject matter at issue was privileged. *See El-Masri*, 479 F.3d at 308, 311 (defining the "central facts" and "very subject matter" of an action as "those facts that are essential

The executive branch has at times acknowledged concerns over the potential abuse of the privilege.[115] Due to concerns that the Bush administration overused the state secrets privilege to stymie national security accountability, the Obama administration reviewed Bush-era claims of the state secrets privilege and drafted a new policy guiding the invocation of the privilege.[116] Under these new guidelines, an internal review group examines privilege requests and makes a recommendation to the attorney general, who must, in writing, approve the privilege claim.[117] Under these guidelines, invocation is appropriate "only when genuine and significant harm to national defense or foreign relations is at stake and only to the extent necessary to safeguard those interests."[118]

The Obama administration's efforts were also an attempt to stave off a renewed congressional push to regulate the privilege by statute.[119] The "State Secrets Protection Act" (SSPA), originally introduced in 2008, would have created several procedural requirements for the invocation and assessment of a state secrets privilege claim.[120] These

---

to prosecuting the action or defending against it"). In other cases, courts found that the privilege prohibited discovery of documents necessary to make a prima facie case and establish standing. *See Al-Haramain*, 507 F.3d at 1205–06 (finding that because the state secrets privilege protected the document upon which Al-Haramain had relied to establish standing, Al-Haramain's claims had to be dismissed unless FISA preempted the state secrets privilege). Many courts remain hesitant to reject the government's invocation of the privilege even as time passes and officials share information about the programs' existence. *See El-Masri*, 479 F.3d at 311 & n.5 (refraining from opining on whether the state secrets privilege would apply to publicly reported information concerning El-Masri's alleged rendition). *But see Husayn*, 938 F.3d at 1134 (9th Cir. 2019) (rejecting the government's blanket assertion of the privilege).

115. SAVAGE, *supra* note 66, at 421–24.

116. *See id.*

117. Memorandum from Eric Holder, U.S. Att'y Gen., to Heads of Executive Departments & Agencies (Sept. 23, 2009), http://www.usdoj.gov/opa/documents/state-secret-privileges.pdf [https://perma.cc/3VY6-TLNU].

118. *Id.*; SAVAGE, *supra* note 66, at 423–24.

119. SAVAGE, *supra* note 66, at 423 (summarizing proposed legislation led by Senator Leahy and Representative Nadler).

120. *See generally* State Secrets Protection Act, S. 2533, 110th Cong. § 4055 (2008). The SSPA's provisions drew expressly from two prominent legislative acts regulating the handling of national security matters and secret information—the Classified Information Procedures Act (CIPA) and the Freedom of Information Act (FOIA). *See* Classified Information Procedures Act, Pub. L. No. 96-456, 94 Stat. 2025 (1980) (codified as amended at 18 U.S.C. App. III); Freedom of Information Act, 5 U.S.C. § 552 (2018). CIPA governs the use of classified information in criminal proceedings and sets forth *in camera*, *ex parte* procedures for reviewing such information under

requirements would have included mandatory review of the materials covered by the invocation of the privilege and a de novo determination by the court with respect to the risks of disclosure.[121] The Obama administration implemented its new policy guidance, which was in part designed to "reduce public cynicism about the privilege," and quietly opposed the SSPA.[122] Since then, efforts to regulate the privilege have waned. Federal lawmakers last introduced the SSPA in 2016, but as recently as 2020, sponsors have indicated that they may reintroduce the SSPA.[123] While attempts to legislatively regulate the state secrets privilege have stalled for the time being, years of electronic surveillance litigation have yielded a potential avenue for plaintiffs through the judicial system, albeit one with its own obstacles.

3. FISA preemption in electronic surveillance litigation

Unlike in the CIA state secrets cases, plaintiffs in electronic surveillance cases have relied on a theory of preemption rooted in FISA.[124] Under this theory, Congress displaced the common law state secrets privilege in electronic surveillance cases when it enacted FISA, which includes *in camera*, *ex parte* procedures to determine the lawfulness of electronic surveillance.[125]

However, beyond establishing that FISA preempts the privilege, plaintiffs in electronic surveillance suits face another obstacle:

---

certain circumstances. 18 U.S.C. App. III, § 6. Under FOIA, the government may withhold information from disclosure under the Act's national security exemption, but courts are authorized to review *de novo* whether the government has properly classified information. 5 U.S.C. §§ 552(a)(4)(B), 552(b)(7).

121. S. 2533, 110th Cong. § 4055 (2008).

122. SAVAGE, *supra* note 66, at 423.

123. *See* Press Release, Jerry Nadler, Chairman, House Comm. on the Judiciary, Chairman Nadler Issues Statement on Attorney General Barr and ADNI Grenell Invocation of 'State Secrets' Doctrine, (Apr. 20, 2020), https://nadler.house.gov/news/documentsingle.aspx?DocumentID=394264 [https://perma.cc/3MWY-DN6A] (criticizing the Trump administration's use of the state secrets privilege in a lawsuit against the Kingdom of Saudi Arabia arising out of 9/11 and noting Rep. Nadler's intent to reintroduce the SSPA).

124. *See, e.g.*, Al-Haramain Islamic Found. v. Bush, 451 F. Supp. 2d 1215 (D. Or. 2006), *rev'd*, 507 F.3d 1190 (9th Cir. 2007) (the first in a series of cases brought by Al-Haramain arguing for FISA preemption).

125. *See, e.g.*, Fazaga v. FBI, 965 F.3d 1015, 1039–40 (9th Cir. 2020) (noting that the only two district courts to consider this issue had both found preemption), *cert. granted*, No. 20-828, 2021 WL 2301971 (U.S. June 7, 2021).

standing.[126] Standing can pose a potentially insurmountable obstacle to plaintiffs seeking redress for harm arising out of surveillance and other national security programs.[127] Given the continued obstacle standing poses in these cases, plaintiffs have sought to pierce the veil of the state secrets privilege to uncover sufficient factual evidence to avoid dismissal.

Plaintiffs began arguing for FISA preemption in the early years of the War on Terror. In 2006, Al-Haramain Islamic Foundation brought a civil suit challenging the TSP after the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC) inadvertently disclosed to Al-Haramain a document indicating that the NSA had surveilled the foundation.[128]

Relying on the Ninth Circuit's decision in *Kasza v. Browner*,[129] Al-Haramain argued that FISA displaces the state secrets privilege in

---

126. One of the bedrock principles of the U.S. judicial framework is that a plaintiff must have standing to bring a cause of action. Antonin Scalia, *The Doctrine of Standing as an Essential Element of the Separation of Powers*, 17 SUFFOLK U. L. REV. 881, 881 (1983). Standing requires that (1) the plaintiff suffered an injury in fact, i.e., one that is sufficiently "concrete and particularized" and "actual or imminent, not conjectural or hypothetical"; (2) the injury is "fairly traceable" to the challenged conduct; and (3) the injury is "likely" to be "redressed by a favorable decision." Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992) (internal quotations omitted). To establish injury-in-fact, the injury must either be "certainly impending" or "based on a substantial risk that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013) (internal quotations and citation omitted). According to the Supreme Court, the standing doctrine performs two key functions: it helps ensure that cases are properly adversarial and diligently argued, and it also prevents the judiciary from "being used to usurp the powers of the political branches." *Id.* at 408.

127. *See Clapper*, 568 U.S. at 408–09; Vladeck, *supra* note 10, at 1042–45 (detailing how *Clapper* may foreclose many avenues for challenging section 702 surveillance); Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 518 (2015) ("Precisely because much modern-day surveillance is covert, this demanding standing test may be impossible to meet. If so, unconstitutional surveillance programs may be immune from judicial review.").

128. Lee Tien, *Litigating the State Secrets Privilege*, 42 CASE W. RES. J. INT'L L. 675, 680 (2010); *Al-Haramain*, 451 F. Supp. 2d at 1229. S*ee generally* Tien, *supra*, at 677, 680–87 (2010) (detailing Al-Haramain's progression through the courts and its FISA preemption theory). The United States had designated Al-Haramain as a "specially designated global terrorist." *Al-Haramain*, 451 F. Supp. 2d at 1218 (noting that OFAC publishes a list of terrorists whose assets are blocked and who are blocked from transacting with U.S. persons).

129. 133 F.3d 1159 (9th Cir. 1998). In *Kasza*, the Ninth Circuit found that because the state secrets privilege is an evidentiary privilege rooted in federal common law, the method to determine if a statute preempts the state secrets privilege "is whether the

surveillance cases because FISA speaks directly to the question of management of national security information in litigation and provides courts with sufficient power to create procedures for the protection of national security interests.[130] Further, Al-Haramain claimed that it would qualify as an aggrieved person—even under the government's theory that FISA's § 1806(f) provisions only apply to aggrieved persons to whom surveillance has been made known—because OFAC had inadvertently shared precisely such evidence.[131]

On interlocutory appeal, the Ninth Circuit held that the district court had correctly refused to dismiss on state secrets grounds because the state secrets privilege did not cover the very subject matter of Al-Haramain's challenge.[132] However, after conducting its own *in camera* review, the Ninth Circuit found that the privilege protected the sealed document Al-Haramain relied upon to establish standing, but remanded the case to the district court with instructions to hear argument on the FISA preemption issue.[133]

On remand in *In re NSA Telecommunications Records Litigation*,[134] the district court agreed with Al-Haramain that FISA preempts the state secrets privilege in electronic surveillance litigation.[135] However, the court found that even though FISA appeared to displace the privilege for purposes of Al-Haramain's claims, Al-Haramain still needed to show that it was an "aggrieved person" within the meaning of FISA.[136]

---

statute '[speaks] directly to [the] question' otherwise answered by federal common law.'" *Id.* at 1167 (latter two alterations in original) (quoting County of Oneida v. Oneida Indian Nation, 470 U.S. 226, 236–37 (1985) (emphasis omitted)).

130. Plaintiffs' Memorandum in Opposition to Defendants' Motion to Dismiss at 7–8, *Al-Haramain*, 451 F. Supp. 2d 1215 (No. CV-06-274). Al-Haramain also analogized its case to Halpern v. United States, 258 F.2d 36 (2d Cir. 1958), where the Second Circuit rejected a claim of privilege in a dispute between a patent inventor and the government under the Invention Secrecy Act. Plaintiffs' Memorandum in Opposition to Defendants' Motion to Dismiss, *supra*, at 8; *Halpern*, 258 F.2d at 44.

131. Plaintiffs' Memorandum in Opposition to Defendants' Motion to Dismiss, *supra* note 130, at 7 n.4.

132. Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1198 (9th Cir. 2007). In particular, the Ninth Circuit based its finding on two sets of facts: (1) that the Bush administration had publicly acknowledged the surveillance program, and (2) that Al-Haramain was officially declared by the government as a "Specially Designated Global Terrorist." *Id.*

133. *Id.* at 1193, 1205–06.

134. 564 F. Supp. 2d 1109 (N.D. Cal. 2008).

135. *Id.* at 1111.

136. *Id.*

Therefore, the court dismissed the FISA claims without prejudice with leave to amend.[137]

In the wake of Al-Haramain's litigation efforts, other plaintiffs brought suit under a FISA preemption theory.

4. The Ninth Circuit endorses FISA preemption

In 2020, the Ninth Circuit became the first federal appellate court to hold that FISA displaces the state secrets privilege in electronic surveillance cases, regardless of whether the case arises under FISA.[138] In *Fazaga*, three Muslim men in California claimed that the FBI violated their constitutional rights by paying a confidential informant to surveil them solely because they were Muslim.[139] In addition to using a confidential informant, the FBI installed electronic surveillance equipment in at least eight mosques in the area.[140] The FBI used this equipment to monitor the plaintiffs' conversations, including those held in offices and other private parts of the mosques.[141] Although the FBI had disclosed some information about the informant's actions, including that he created audio and video recordings and provided handwritten notes to the FBI, the government asserted the privilege over three categories of evidence: (1) information confirming or denying whether any particular individual was a target of an investigation; (2) information relating to the predicate for any such investigation, any information gathered as a result, and the status of

137. *Id.* at 1137.

138. *See* Fazaga v. FBI, 965 F.3d 1015, 1044 (9th Cir. 2020).

139. *Id.* at 1024. Craig Monteilh, one of more than 15,000 confidential informants recruited by the FBI after 9/11, spent eighteen months secretly recording conversations and providing intelligence to the FBI. Trevor Aaronson, *Spy in Disguise: An FBI Informant's Unlikely Role in Upcoming Supreme Court Case on Surveillance of Muslims*, INTERCEPT (Sept. 12, 2021, 6:00 AM), https://theintercept.com/2021/09/12/fbi-informant-surveillance-muslims-supreme-court-911 [https://perma.cc/TWK9-6ENV]. As part of his mission, Monteilh "encouraged people to visit 'jihadist' websites . . . and sought to obtain compromising information that could be used to pressure others to become informants." *Fazaga*, 965 F.3d at 1026–27. Eventually, his FBI handlers instructed Montielh to "begin more pointedly asking questions about jihad and armed conflict and to indicate his willingness to engage in violence." *Id.* at 1027. However, the local mosque leadership—disturbed by Monteilh's behavior—reported him to the FBI and filed a restraining order. *Id.* at 1027–28. After spending eight months in prison for his involvement in a con scheme, Monteilh and the FBI reportedly had a falling out and in 2008, Monteilh "blew the whistle" on Operation Flex. Aaronson, *supra*.

140. *Fazaga*, 965 F.3d at 1027.

141. *Id.*

investigation; and (3) information relating to sources or methods.[142] As a result, the government argued that a number—but not all—of the plaintiffs' claims should be dismissed under *Reynolds*.[143]

In its denial of rehearing en banc, the Ninth Circuit affirmed that the *Reynolds* privilege is a federal common law evidentiary privilege; therefore, to displace the state secrets privilege, Congress need not affirmatively preempt it, but merely "speak directly" to the question addressed by the privilege.[144] The Ninth Circuit reviewed the relevant FISA civil remedy provisions and found that the plaintiffs had alleged a FISA claim against individual government agents for recordings made by devices planted by FBI agents in the home of one plaintiff and the office of another.[145]

The Ninth Circuit held that FISA's plain language, statutory structure, and legislative history demonstrate that Congress intended FISA to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance.[146] The Ninth Circuit followed circuit precedent from *Kazsa* in finding that FISA "speaks directly" to the same circumstances as the privilege.[147] After finding that the same concerns underlying the privilege animated § 1806(f)'s procedures, the Ninth Circuit emphasized FISA's legislative history—and Congress's discussion of the prior common law system's failure to appropriately balance national security and prevent abuse—militated in favor of preemption.[148]

The Ninth Circuit further found that an aggrieved person challenging electronic surveillance in a civil suit may use FISA's § 1806(f) procedures, whether the challenge is under FISA itself, the Constitution, or any other law.[149] The Ninth Circuit reasoned that § 1806(f)'s procedures applied for two reasons: first, the plaintiffs

142. *Id.* at 1029.

143. *Id.*

144. *Id.* at 1044 (first citing City of Milwaukee v. Illinois, 451 U.S. 304 (1981); then citing United States v. Texas, 507 U.S. 529 (1993)).

145. *See id.* at 1032, 1038–39 (finding that claims based on all other categories of surveillance failed because "the Agent Defendants either did not violate FISA; are entitled to qualified immunity on the FISA claim because Plaintiffs' reasonable expectation of privacy was not clearly established; or were not plausibly alleged in the complaint to have committed any FISA violation that may have occurred").

146. *Id.* at 1052.

147. *Id.* at 1045. The Ninth Circuit rejected the government's argument for a more exacting "clear statement" standard. *Id.* at 1044.

148. *See id.* at 1047.

149. *Id.* at 1051–52.

alleged that the information covered by the government's invocation of the privilege was obtained or derived from FISA-covered electronic surveillance;[150] and second, the plaintiffs had requested to obtain information under FISA via injunctive relief, including ordering the destruction or return of any information gathered under the electronic surveillance program.[151]

The Ninth Circuit also noted that it was not the first court to find that § 1806(f)'s procedures could be used outside the context of claims under § 1810.[152] In *ACLU Foundation of Southern California v. Barr*,[153] the plaintiffs sought declaratory and injunctive relief against then-Attorney General Barr and other federal officials for allegedly unlawful surveillance.[154] The United States invoked § 1806(f) in response to several of the plaintiffs' motions in deportation proceedings to discover electronic surveillance and to suppress the use of that information.[155] The district court judge conducted an *in camera*, *ex parte* review and determined that the electronic surveillance was lawful, and the plaintiffs appealed.[156] The D.C. Circuit, in upholding the district court's *in camera*, *ex parte* review, emphasized that when a court conducts a § 1806(f) review, "its task is not simply to decide whether the surveillance complie[s] with FISA," but whether it complies with the Constitution.[157] Relying on *Barr*, the Ninth Circuit in *Fazaga* found it could properly apply § 1806(f)'s procedures to the case at issue.[158]

Finally, because one plaintiff had a reasonable expectation of privacy in his office and another plaintiff had a reasonable expectation of privacy in his home, car, and phone, the Ninth Circuit considered

---

150. *Id.* at 1049.

151. *Id.* (emphasizing that the panel was proceeding on the premise that the Attorney General's invocation of the state secrets privilege relied on the potential use of material obtained or derived from electronic surveillance, as alleged in the complaint, but should that not be the case, the district court could decide that the FISA procedures were inapplicable on remand).

152. *Id.* at 1052.

153. 952 F.2d 457 (D.C. Cir. 1991).

154. *Id.* at 460. Plaintiffs claimed that the government had violated § 1805(a)(2)(A), which required certain stringent procedures before surveilling a U.S. person solely on the basis of their First Amendment activities. *See* 50 U.S.C. § 1805(a)(2)(A).

155. *ACLU Found. of S. Cal.*, 952 F.2d at 463.

156. *Id.*

157. *Id.* at 465.

158. *See* Fazaga v. FBI, 965 F.3d 1015, 1052 (9th Cir. 2020), *cert. granted*, 2021 WL 2301971 (U.S. June 7, 2021) (No. 20-828).

them aggrieved persons as to those categories of surveillance.[159] The panel affirmed in part and reversed in part the district court's orders and remanded for further proceedings.[160] On remand, the panel instructed the district court to use § 1806(f)'s *in camera, ex parte* procedures to review any materials relating to the surveillance as may be necessary, including the evidence over which the attorney general asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted.[161] In a concurring opinion, Judge Berzon sought to limit the scope of the panel opinion, emphasizing that it had merely "concluded that . . . § 1806(f)[] supersedes the common law state secrets evidentiary privilege's limited dismissal remedy—not the protection of state secrets from disclosure" and that they apply here.[162]

In a stinging rebuke of the majority's analysis, Judge Bumatay—joined by nine other circuit judges—warned against disrupting the balance of powers and "tip[ping] that balance in favor of inventive litigants and overzealous courts, to the detriment of national security."[163] In Judge Bumatay's view, the state secrets privilege is not a mere common law evidentiary privilege but rather an outgrowth of the executive power and the President's authority as Commander in Chief.[164] Judge Bumatay relied in large part on the Fourth Circuit's decision in *El-Masri v. United States*,[165] in which the court dismissed an

159. *Id.* at 1053.

160. *Id.* at 1068.

161. *Id.* at 1065. As noted above, the government filed a petition for certiorari in late 2020, and the United States Supreme Court granted in June 2021. FBI v. Fazaga, 2021 WL 2301971 (U.S. June 7, 2021) (No. 20-828).

162. *Fazaga*, 965 F.3d 1015 at 1068 (Berzon, J., concurring).

163. *Id.* at 1074 (Bumatay, J., dissenting) (positing that, after *Fazaga*, "litigants can dodge the state secrets privilege simply by invoking 'electronic surveillance' somewhere within the Ninth Circuit," and in defending itself, "the government may be powerless to prevent the disclosure of state secrets").

164. *Id.* at 1073, 1076. Judge Bumatay relied on Professor Chesney's exploration of the privilege's origins. *See* Chesney, *supra* note 31, at 1270–71 (noting that mid-nineteenth century treatise writers, in seeking to rationalize and systematize common law evidentiary rules, wove many of these cases together under a broader "public interest" privilege); *see also* Zagel, *supra* note 89, at 880 ("The *sine qua non* of the state secrets privilege is that the public interest is served."). However, while treatise writers had begun referring expressly to a "state secrets privilege" by the late nineteenth century, it was not until much later that the modern privilege—with its core focus on military and diplomatic secrets—emerged. *See* Chesney, *supra* note 31, at 1281.

165. 479 F.3d 296 (4th Cir. 2007)

action arising out of the CIA's extraordinary rendition program under the state secrets privilege.[166] In *El-Masri*, the Fourth Circuit noted that while the state secrets privilege was developed at common law, "it performs a function of constitutional significance[] because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities."[167]

In his *Fazaga* dissent, Judge Bumatay also referenced several formative cases for the proposition that "modern courts have recognized the Article II dimension of executive privileges."[168] In *United States v. Nixon*,[169] the Court cited *Reynolds* in stating that, to the extent a privilege relates to the "effective discharge of a President's powers, it is constitutionally based."[170] Similarly, in *Department of Navy v. Egan*,[171] the Court assessed a suit arising out of the revocation of a security clearance and found that the President's Article II authority extends to protecting information bearing on national security, including by classification and controlling access to such information.[172] Quoting Justice Jackson's opinion in *Chicago & Southern Air Lines, Inc. v. Waterman Steamship Corp.*,[173] Judge Bumatay wrote that "[t]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services

166. *See id.* at 311. El-Masri, a German citizen of Lebanese descent, alleged that he had been illegally detained, tortured, and subjected to other inhumane treatment as part of the CIA's extraordinary rendition program. *See id.* at 300. While many details of the CIA's rendition program were—and remain—highly classified, news media and government officials disclosed the existence of and some details about the program. *See id.* at 301–02. Nonetheless, the United States intervened as a defendant in the district court, asserting that the civil action could not proceed because it posed an unreasonable risk of disclosing state secrets. *Id.* at 301.

167. *Id.* at 303–04 (emphasizing that the privilege "has a firm foundation in the Constitution, in addition to its basis in the common law of evidence"). The Fourth Circuit also noted that the Court in *Reynolds* suggested that "the state secrets doctrine allowed the Court to avoid the constitutional conflict that might have arisen had the judiciary demanded that the Executive disclose highly sensitive military secrets." *Id.* at 303.

168. Fazaga v. FBI, 965 F.3d 1015, 1077 (9th Cir. 2020) (Bumatay, J., dissenting), *cert. granted*, 2021 WL 2301971 (U.S. June 7, 2021) (No. 20-828).

169. 418 U.S. 683 (1974).

170. *Id.* at 711.

171. 484 U.S. 518 (1988).

172. *Id.* at 527 (citing United States. v. Reynolds, 345 U.S. 1 (1953); Totten v. United States, 92 U.S. 105 (1875)).

173. 333 U.S. 103 (1948).

whose reports neither are nor ought to be published to the world."[174] Judge Bumatay contrasted the state secrets privilege's "broad constitutional design" with FISA's "limited function."[175]

Judge Bumatay further argued that, even if FISA displaced the privilege, § 1806(f)'s procedures apply only when the government tries to affirmatively use such evidence or when a surveilled party attempts to suppress the evidence.[176] Finally, Judge Bumatay emphasized the risks of disclosing state secrets, characterizing the panel's decision as one that will command courts to disclose evidence to plaintiffs.[177]

5. The current stage of NSA surveillance litigation

Fazaga immediately provided support for plaintiffs in several NSA surveillance cases, which had been making their way through the courts for much of the previous decade.

In *Jewel v. NSA*,[178] a group of plaintiffs filed a class action to redress injuries resulting from NSA surveillance.[179] In support of their claims, the plaintiffs relied on documents provided by a former AT&T employee purporting to show that the company had routed copies of communication information to an NSA-controlled secure facility in AT&T's San Francisco office.[180] After initially being dismissed on standing, the Ninth Circuit reversed, finding that the plaintiffs had

---

174. Fazaga v. FBI, 965 F.3d 1015, 1077 (Bumatay, J., dissenting) (quoting *Waterman*, 333 U.S. at 111), *cert. granted*, 2021 WL 2301971 (U.S. June 7, 2021) (No. 20-828). *Waterman* involved a petition for judicial review of an order of the Civil Aeronautics Board under the Civil Aeronautics Act (CAA). 333 U.S. at 104. In dicta, Justice Jackson emphasized that it would be intolerable to allow courts, without the information properly held secret, to review and potentially nullify executive action. *Id.* at 111. Further, Justice Jackson noted that the CAA did not provide an *in camera* mechanism for review. *Id.*

175. *Fazaga*, 965 F.3d at 1073 (Bumatay, J., dissenting).

176. *Id.*

177. *Id.* In *El-Masri*, the Fourth Circuit also addressed El-Masri's contention that, in lieu of dismissal, the district court could have employed an alternative *in camera* procedure, which would have allowed El-Masri, his counsel, and the court to review the privileged material. *See* El-Masri v. United States, 479 F.3d 296, 311 (4th Cir. 2007). However, the court rejected this claim, citing *Reynolds* for the proposition that once a court determines that a claim of privilege is appropriate, it should not jeopardize those secrets by conducting any form of examination of those materials, even *in camera*. *Id.* (quoting United States v. Reynolds, 345 U.S. 1, 10 (1953)).

178. No. C 07-0693, 2010 WL 235075 (N.D. Cal. Jan. 21, 2010), *rev'd*, 673 F.3d 902 (9th Cir. 2011).

179. *Id.* at *4–5.

180. *Id.* at *5.

sufficiently alleged a concrete and particularized injury; however, it remanded the case to the district court to decide whether the state secrets privilege barred further litigation.[181]

On remand, in 2013, the district court granted the plaintiffs' motion for summary adjudication, finding that FISA's § 1806(f) procedures displace the state secrets privilege, allowing some of the plaintiffs' non-statutory claims to move forward.[182] However, in 2015, the district court ultimately granted the government's motion for summary judgment because the plaintiffs lacked standing and the state secrets privilege precluded their claims.[183] In doing so, the district court relied on *Clapper v. Amnesty International USA*,[184] where the Supreme Court dismissed a challenge to the section 702 program by attorneys and human rights, labor, legal, and media organizations.[185] The *Clapper* Court found the plaintiffs had not established standing and that an injury must be *certainly impending*, not merely possible, to establish standing.[186]

In *Jewel*, the district court found that the plaintiffs—unlike those in *Clapper*—had provided evidence sufficient to establish that their

---

181. Jewel v. NSA, 673 F.3d 902, 910–13 (9th Cir. 2011) (emphasizing that "procedural, evidentiary and substantive barriers" may prove fatal to the plaintiffs' standing).

182. Jewel v. NSA, 965 F. Supp. 2d 1090, 1104 (N.D. Cal. 2013).

183. *Jewel*, Nos. C 08-04373 & C 07-00693, 2015 WL 545925, at *1 (N.D. Cal. Feb. 10, 2015), *appeal dismissed and remanded*, 810 F.3d 622 (9th Cir. 2015).

184. 568 U.S. 398 (2013).

185. *Id.* at 406, 408.

186. *Id.* at 422. The plaintiffs in *Clapper* claimed that the government had presumably collected their communications because they engaged in sensitive international communications with likely targets of the surveillance program. *Id.* at 406–07. Justice Alito, writing for the Court, stated that these concerns were "highly speculative" and reliant "on a highly attenuated chain of possibilities." *Id.* According to the Justice Alito, this "chain of possibilities" included the following links: (1) the speculative nature of whether the government would immediately target communications to which respondents were parties, given the lack of knowledge at that time about the NSA's targeting practices; (2) that even if respondents made such a demonstration, it was pure speculation as to whether the government would use the section 702 authorities—as opposed to other surveillance authorities—to do so; (3) that even if both of the first two prongs were met, it was speculative to assume the FISC would authorize such surveillance; (4) that even if approved, there was no evidence corroborating the assumption that the government would succeed in acquiring the communications of respondents' foreign contacts; and (5) that even in the event the government successfully acquired such communications, it was pure speculation to suggest that the government would incidentally have acquired respondents' own communications. *Id.*

communications would be captured in a dragnet internet collection program if such a program operated as plaintiffs alleged.[187] However, the district court found the plaintiffs had provided insufficient evidence to establish that the Upstream collection process operated in the manner described by the plaintiffs.[188]

After yet another reversal by the Ninth Circuit, the district court permitted discovery on the remaining standing claims and reviewed the government's classified declaration and accompanying documents, ordering both parties to move for summary judgment on standing.[189] The district court then granted the government's motion and dismissed all claims on standing and state secrets privilege grounds.[190]

In dismissing the case, the district court first found that the plaintiffs had not proffered sufficient admissible evidence to establish standing.[191] Further, the court found that even if the plaintiffs had done so, further adjudication could not proceed "without risking exceptionally grave damage to national security."[192] In particular, the court emphasized that, based on its "extensive *in camera* review of the classified materials," it could not issue a judgment—whether on standing or on the merits—without exposing classified information.[193] After finding that the state secrets privilege was properly invoked, the district court found that it must dismiss the case.[194] In doing so, it distinguished *Jewel* from *Fazaga* in two ways: (1) that *Fazaga* had not addressed the question of what courts should do when "the answer to the question of whether a particular plaintiff was subjected to surveillance—i.e., is an "aggrieved person" under § 1806(f)—is the very information over which the Government seeks to assert the state secrets privilege"; and (2) that unlike in *Fazaga*—and any other state secrets case known to the court—the district court had conducted a comprehensive review of the classified information prior to dismissal.[195]

---

187. *Jewel*, 2015 WL 545925, at *4.
188. *Id.*
189. Jewel v. NSA, No. C 08-04373, 2019 WL 11504877, at *3 (N.D. Cal. Apr. 25, 2019), *aff'd*, No. 19-16066, 2021 WL 3630222 (9th Cir. Aug. 17, 2021).
190. *See id.* at *13–14.
191. *Id.* at *10.
192. *Id.*
193. *Id.* at *11.
194. *Id.* at *14.
195. *Id.* at *12–13.

In August 2021, the Ninth Circuit affirmed, finding that the plaintiffs had failed to sufficiently establish injury in fact.[196] The Ninth Circuit noted that the plaintiffs' argument that they may use § 1806(f) to establish their standing "ignores the fact that it is *their* 'burden to prove their standing *by pointing to specific facts*[.]'"[197] Because the Ninth Circuit agreed with the lower court's ruling on standing, the Ninth Circuit refrained from considering the district court's ruling that the plaintiffs' claims were barred by the state secrets privilege.[198]

Meanwhile, a similar fight was taking place in the Fourth Circuit. In *Wikimedia*, Wikimedia sought an injunction against the NSA's Upstream surveillance program.[199] Wikimedia raised two theories of standing: a "Dragnet Allegation," contending that the NSA was "intercepting, copying, and reviewing substantially all" internet "communications entering and leaving the United States," and a "Wikimedia Allegation" contending that, even if Upstream was not a dragnet, Upstream still copied at least some of Wikimedia's communications.[200] This latter theory of standing rested on three prongs, namely,

> (A) Wikimedia's communications almost certainly traverse every international Internet backbone link connecting the United States

---

196. Jewel v. NSA, No. 19-16066, 2021 WL 3630222, at *1, *2 (9th Cir. Aug. 17, 2021).

197. *Id.* at *1 (citing Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013)); *see also* Transunion LLC v. Ramirez, 141 S. Ct. 2190, 2207 (2021).

198. *Id.*

199. When Wikimedia sought evidence related to the Upstream program, the government invoked the state secrets privilege in response to a number of discovery requests. Wikimedia Found. v. NSA, 427 F. Supp. 3d 582, 591–92 (D. Md. 2019). Daniel Coats, then Director of National Intelligence, asserted the privilege over seven categories of information: "(A) information that would tend to confirm what individuals or entities are subject to Upstream surveillance activities; (B) information concerning the operational details of the Upstream collection process; (C) the location(s) at which Upstream surveillance is conducted; (D) the categories of Internet-based communications collected through Upstream surveillance activities; (E) information concerning the scope and scale of Upstream surveillance; (F) NSA cryptanalytic capabilities; and (G) additional categories of classified information regarding Upstream surveillance contained in opinions and orders issued by, and submissions made to, the [FISC]." Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *3 (Sept. 15, 2021). After Wikimedia sought to compel standing through the use of § 1806(f), the government sought summary judgment on standing or, in the alternative, based on its invocation of the state secrets privilege. *Wikimedia*, 427 F. Supp. 3d at 592–93.

200. *Wikimedia*, 427 F. Supp. 3d at 591–92, 600–01.

> with the rest of the world; (B) the NSA conducts Upstream surveillance one or more points along the Internet backbone; and (C) the NSA, for technical reasons, must be copying and reviewing all the text-based communications that travel across a given Internet backbone link upon which it conducts Upstream surveillance.[201]

The district court found that Wikimedia had established a genuine issue of material fact as to the first two prongs.[202] However, the court found that Wikimedia had failed to meet its burden with regard to the third prong because "the NSA, in the course of Upstream surveillance, does not need to be copying any of Wikimedia's communications as a technological necessity."[203] On the third prong, both parties submitted expert testimony hypothesizing on how the Upstream surveillance program functions.[204] However, the district court determined that Wikimedia's expert testimony was inadmissible because its expert had no knowledge of the Upstream surveillance program's actual operation; thus, the expert based his testimony on "speculative assumptions about the NSA's surveillance practices and priorities and the NSA's resources and capabilities."[205] Further, the court found that, even if Wikimedia's expert testimony was admissible, the state secrets privilege would bar any conclusions drawn from those inferences.[206]

While Wikimedia's failure to meet its burden in establishing its allegation was dispositive, the district court nonetheless proceeded to

---

201. *Id.* at 600–01.

202. *Id.* at 601–03 (noting that the NSA did not dispute the first prong and that the former Director of National Intelligence Dan Coats's admissions, combined with a 2011 redacted FISC opinion and the PCLOB's 702 report, sufficed to meet the second prong).

203. *Id.* at 601, 603 n.41 (noting that instead of attempting to establish standing along the lines of *Clapper*, Wikimedia chose argued it was technologically impossible for the NSA not to have copied or scanned Wikimedia communications under the Upstream surveillance program). However, on appeal, Wikimedia argued that the district court erroneously imposed a higher standard of pleading, and that Wikimedia had presented evidence pointing to both the NSA's surveillance of Wikimedia's communications as a technological necessity and as a virtual certainty. Brief for Plaintiff-Appellant, at 37–38, Wikimedia Found. v. NSA, No 20-1191, 2021 WL 4187840 (4th Cir. Sept. 15, 2021).

204. *Wikimedia*, 427 F. Supp. 3d at 603–04.

205. *Id.* at 604–05. On appeal, Wikimedia challenged the district court's admissibility finding under Daubert v. Merell Dow Pharms., Inc., 509 U.S. 579 (1993). *See* Brief for Plaintiff-Appellant, *supra* note 203, at 41. *Daubert*'s application to covert surveillance litigation is beyond the scope of this Comment.

206. *Wikimedia*, 427 F. Supp. 3d at 605.

analyze the state secrets privilege and found that any further litigation regarding Wikimedia's standing would require the disclosure of state secrets.[207] Finally, the district court rejected Wikimedia's § 1806(f) argument, finding that Wikimedia had not established a genuine dispute of material fact concerning its status as an aggrieved person under FISA.[208] Therefore, the court found dismissal appropriate.[209] In rejecting Wikimedia's § 1806(f) argument, the court emphasized that, on its face, § 1806(f) persuasively indicates that Congress intended these procedures to apply "only after it became clear from the factual record that the [plaintiff] was the subject of electronic surveillance."[210]

On appeal again, the Fourth Circuit affirmed on state secrets grounds in a divided panel opinion.[211] After finding that the district court erred in granting summary judgment as to Wikimedia's standing, the Fourth Circuit agreed that the state secrets privilege required dismissal.[212]

Addressing standing, the Fourth Circuit found that Wikimedia had established a genuine issue for trial on the second prong of the Wikimedia allegation: that Upstream surveillance takes place on at least one international internet link.[213] The Fourth Circuit also found that Wikimedia had established a genuine issue for trial on the third prong of the Wikimedia allegation: that the NSA copies all communications on a monitored link.[214] However, the Fourth Circuit then held that the state secrets privilege foreclosed any further litigation.[215] In doing so, the panel concluded that § 1806(f)'s

---

207. *Id.* at 610, 613 ("Even if Wikimedia could establish a *prima facie* case of its standing based solely on the public, unclassified record, which it has not been able to do thus far in this case, the state secrets doctrine still requires dismissal because the defendants cannot properly defend themselves without using privileged evidence.").

208. *Id.*

209. Wikimedia raised several additional standing arguments unrelated to the Wikimedia Allegation, all of which the district court rejected. *See id.* at 616.

210. *Id.* at 614 (quoting Wikimedia Found. v. NSA, 335 F. Supp. 3d 772, 781 (D. Md. 2018)).

211. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *1 (4th Cir. Sept. 15, 2021).

212. *Id.*

213. *Id.* at *9–12.

214. *Id.* at *12–13. Unlike at the motion to dismiss phase, Wikimedia argued that the NSA was *choosing* to copy all communications on a monitored, rather than copying by technical necessity. *Id.* at *12.

215. *Id.* at *14.

procedures are relevant "only when a litigant challenges the admissibility of *the government's* surveillance evidence."[216]

At the outset, the Fourth Circuit acknowledged the ambiguity of its own prior decisions addressing the nature of the state secrets privilege.[217] Nonetheless, the panel chose not to resolve that ambiguity, instead finding that even if the privilege was rooted in the common law, FISA does not "speak directly" to the situation in *Wikimedia*.[218]

The Fourth Circuit, relying on several canons of statutory construction, found that the third condition triggering *in camera*, *ex parte* review—the aggrieved person's motion or request 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" must be construed narrowly to include only those instances where the government seeks to use such evidence in a civil or criminal proceeding.[219] Relying on the principles of *noscitur a sociis*[220] and *esjudem generis*,[221] Judge Diaz found that because both of the other conditions in § 1806(f) relate to the government's introduction of evidence derived from surveillance, the subsequent reference to "any" motion or request must be construed to include only those motions or requests "contingent on the government's use of surveillance evidence."[222] According to Judge Diaz, those same canons of construction cabin the meaning of "other material" and "such other material" to include only "documents related to officially approving and defining the scope of FISA

---

216. *Id.* (emphasis added). Judge Motz took issue with the panel's decision to publish an opinion prior to the Supreme Court's decision in *Fazaga*. *Id.* at *24 (Motz, J., concurring in part and dissenting in part).

217. *Id.* at *15 (majority opinion) (noting that *El-Masri* mentioned both the rule's basis in the law of evidence, but also that it performs a function of constitutional significance).

218. *Id.* (quoting United States v. Texas, 507 U.S. 529, 534 (1993)).

219. *Id.* at *16–17. Judge Diaz assumed Wikimedia was an aggrieved person and therefore did not address what a plaintiff must prove to establish their status as an aggrieved person. *Id.* at *16 n.15.

220. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 195 (2012) ("Associated words bear on one another's meaning . . . .").

221. *See id.* at 199 ("Where general words follow an enumeration of two or more things, they apply only to persons or things of the same general kind or class specifically mentioned . . . .").

222. *Id.* at *16.

surveillance that can thus be used to determine the legality of the government's surveillance operations."[223]

Judge Diaz also relied on the structure of § 1806 and FISA more generally to rebut reading § 1806(f) as a "free-floating right" to obtain evidence relating to surveillance.[224] Judge Diaz found that the "paradigmatic remedy" for a finding of unlawful surveillance under § 1806(f) is the suppression of evidence, not Wikimedia's desired remedy—having the court conduct an *in camera*, *ex parte* review in order to decide Wikimedia's standing and merits of its claims.[225]

Responding to Wikimedia's argument that rejecting FISA preemption would in effect give the government control of legal challenges to its surveillance programs, Judge Diaz stressed the protections inherent in the *Reynolds* doctrine, as well as the FISC's *ex ante* review of surveillance programs.[226] Therefore, Judge Diaz concluded, this narrower reading of § 1806(f) is "entirely consistent with ensuring judicial review of executive branch surveillance."[227] Judge Diaz further emphasized that reading § 1806(f) this way did not render FISA's civil remedy useless in cases where the government has not provided notice.[228] Rather, according to Judge Diaz, Congress intended to create a civil remedy applicable even in situations where the government has not complied with its duty to notify a litigant when it intends to use evidence derived from surveillance.[229] Finally, Judge Diaz found that incongruences between § 1806(f) and the state secrets privilege militated in favor of rejecting Wikimedia's preemption argument.[230]

After finding that the government had appropriately invoked the state secrets privilege, Judge Diaz declined to endorse Wikimedia's argument that, before dismissing a case based on the government's assertion that it cannot defend itself without privileged information, the court should conduct an *in camera*, *ex parte* review to "determine the validity—or at least the existence of the government's hypothetical

223. *Id.* at *17.
224. *Id.* at *16; *see id.* at *17–18 (analyzing the structure of § 1806 and surrounding provisions).
225. *Id.* at *17.
226. *Id.* at *19–20.
227. *Id.* at *20.
228. *Id.* at *18.
229. *Id.*
230. *Id.* at *19.

defense."[231] Judge Diaz contrasted Wikimedia's case to other cases in which the government had asserted a "valid defense" because there is "no conceivable defense" to Wikimedia's claim—that the NSA is acquiring all communications on a chokepoint cable it is monitoring—which would not reveal state secrets.[232] In so finding, Judge Diaz refused to "condone holding a one-sided trial" to determine the merits of Wikimedia's claims.[233] Therefore, Judge Diaz affirmed the district court's holding that the state secrets privilege barred further litigation to support Wikimedia's standing.[234]

Judge Motz, concurring in part and dissenting in part, took issue with both the panel's decision to issue an opinion so close to the Supreme Court's hearing of *Fazaga*, as well as its state secrets analysis.[235] Summarizing her concern, Judge Motz emphasized that the panel opinion marked a departure from *Reynolds* and its progeny, and "stands for a sweeping proposition: A suit may be dismissed under the state secrets doctrine, after minimal judicial review, even when the Government premises its only defenses on far-fetched hypotheticals."[236] The panel opinion, according to Judge Motz, "relegates the judiciary to the role of bit player in cases where weighty constitutional interests ordinarily require us to cast a more 'skeptical eye.'"[237]

In particular, Judge Motz noted that whereas *Reynolds* relied in part on the availability of other evidence, courts have repeatedly viewed *in camera*, *ex parte* procedures as necessary where the government invokes the privilege based on a claim of valid defense.[238] Rejecting Judge Diaz's conclusion that such process was not necessary because the government had sufficiently established that any valid defense would require privileged materials.[239] Judge Motz noted that the government

---

231. *Id.* at *22–23.

232. *Id.* at *23.

233. *Id.*

234. *Id.* Judge Diaz also affirmed the district court's findings on Wikimedia's supplementary theories of standing. *Id.* at *24.

235. *Id.* at *25 (Motz, J., concurring in part and dissenting in part). Circuit Judge Rushing wrote separately to state that he would have held that Wikimedia failed to demonstrate a dispute of material fact regarding its standing. *Id.* at *64 (Rushing, C.J., concurring in part and concurring in the judgment).

236. *Id.* at *25 (Motz, J., concurring in part and dissenting in part).

237. *Id.* (quoting Abilt v. CIA, 848 F.3d 305, 312 (4th Cir. 2017)).

238. *See id.* at *26 (collecting cases).

239. *Id.* at *26–27 (criticizing Judge Diaz for accepting the government's "totally inadequate hypotheticals" and "boilerplate claims of privilege" as valid defenses).

had offered two defenses: (1) that Upstream surveillance might not operate at any international "chokepoint" cables; and (2) that it is hypothetically possible that Upstream operates in a way that avoids Wikimedia's communications.[240] Both Judge Motz and Judge Diaz struggled to reconcile the first defense with the government's public disclosures and "simple common sense."[241] Judge Motz also faulted the government for failing to explain how an "appropriately tailored *in camera* review" could not examine the government's second defense without jeopardizing state secrets.[242] Instead, according to Judge Motz, Judge Diaz and the government endorsed such a broad reading of *Reynolds*, which raises the serious question of whether "*any* electronic surveillance case could *ever* proceed to the merits."[243]

The Ninth Circuit decision in *Fazaga* has provided important support to plaintiffs seeking to challenge surveillance activities, whether by the FBI, NSA, or other government agencies. However, as the most recent decisions in *Jewel* and *Wikimedia* indicate, there remain significant procedural obstacles to judicial redress.[244]

This Comment has explored the development of electronic surveillance and the state secrets privilege to contextualize current efforts to seek redress through Article III courts. The remainder of this Comment will argue that the *Fazaga* court correctly determined that FISA displaced the state secrets privilege in electronic surveillance litigation. It will further argue that FISA's *in camera, ex parte* procedures govern in cases—like those in *Wikimedia* and *Jewel*—where the allegedly privileged material concerns whether a particular plaintiff was subject to surveillance.

II. ANALYSIS

While the Supreme Court has not ruled on whether FISA displaces the state secrets privilege, it has indicated as recently as 2011 that the privilege is an evidentiary one.[245] Considering FISA's text, structure, and legislative history, the Ninth Circuit correctly found in *Fazaga* that

240. *Id.* at *26.
241. *Id.*
242. *Id.*
243. *Id.* at *27.
244. *See, e.g.*, Wikimedia Found. v. NSA, 427 F. Supp. 3d 582, 619–20 (D. Md. 2019) (finding that the judicial branch, rather than the executive branch alone, provides for the review and oversight of unlawful surveillance through limited avenues), *aff'd*, No. 20-1191, 2021 WL 4187840 (4th Cir. Sept. 15, 2021).
245. *See* Gen. Dynamics Corp. v. United States, 563 U.S. 478, 484 (2011).

FISA displaces the state secrets privilege in electronic surveillance litigation.[246] While neither *Fazaga* nor the Fourth Circuit in *Wikimedia* ruled on the precise extent of FISA's reach, these same sources indicate Congress intended to make FISA's *in camera*, *ex parte* procedures available even where the government has invoked the state secrets privilege to prevent access to materials cutting to whether that particular plaintiff was subject to surveillance.

A. FISA § 1806(f) Displaces the State Secrets Privilege in Electronic Surveillance Cases

This Section argues that FISA's § 1806(f) procedures displace the state secrets privilege in NSA surveillance cases like *Wikimedia* and *Jewel*. First, it argues that the Court in *Reynolds* and its progeny has emphasized the privilege's basis in common law evidentiary rules, leaving it open for congressional regulation. Second, this Section analyzes FISA's text, structure, and purpose to find that Congress intended to displace the state secrets privilege in electronic surveillance cases, including affirmative challenges to the lawfulness of a surveillance program. Finally, this Section concludes that these same factors also indicate that Congress intended § 1806(f) to apply in situations where the government invokes the privilege to prevent disclosure of evidence indicating whether a particular plaintiff was subject to surveillance.

1. The state secrets privilege is a federal common law evidentiary privilege

As the Ninth Circuit correctly noted in *Fazaga*, the state secrets privilege is an evidentiary rule rooted in common law, not the Constitution.[247] While the government and some commentators have continued to press for recognition of the state secrets privilege as an outgrowth of Article II executive power that is therefore within the realm of constitutionally based executive privileges, this position is unavailing for several reasons.

First, such a reading of the state secrets privilege is in tension with how scholars initially understood the Court's decision in *Reynolds*. *Reynolds* concerned the government's prerogative to prevent the revelation of military secrets, a privilege that the Court emphasized was "well established in the law of evidence."[248] While the government

246. *See Fazaga*, 965 F.3d at 1040, 1044.
247. *Id.* at 1045.
248. United States v. Reynolds, 345 U.S. 1, 6–7 (1953).

argued for a broader executive power to withhold documents in the public interest, the Court expressly declined to endorse such a view, finding that there was a "narrower ground for decision."[249] Subsequent discussion of *Reynolds* among legal scholars characterized the privilege as evidentiary in nature.[250]

Second, despite some lasting confusion, the state secrets privilege does not fall within the broader remit of constitutionally based executive privilege, although there are certainly overlapping characteristics between the two.[251] In pressing for a constitutional basis for the state secrets privilege, the government has argued, citing broad claims in *Nixon* and *El-Masri*, that while the state secrets privilege developed from common law, "it performs a function of constitutional significance" in allowing the executive branch to protect secret information related to the military and foreign affairs, a function that is in turn rooted in the separation of powers and the Executive's Article II authorities.[252]

This argument conflates the President's unique position with the executive branch's broader interests in maintaining the secrecy of information. In *Nixon*, the Court in dictum referenced *Reynolds* in contrast with the President's general interest in confidentiality.[253] *El-*

---

249. *Id.* at 6.

250. *See* Zagel, *supra* note 89, at 909 (discussing the privilege among other evidentiary privileges available to the government); Note, *Evidence—Three Nonpersonal Privileges*, 29 N.Y.U. L. REV. 194, 194–95 (1954) (discussing the privilege in context of other evidentiary privileges, such as informer privilege and official information privilege); *see also* Milton M. Carrow, *Governmental Nondisclosure in Judicial Proceedings*, 107 U. PA. L. REV. 166, 192 (1958) (distinguishing between claims of privilege by the President and those made by other officials).

251. *See* Zagel, *supra* note 89, at 875–76 (noting that the privileges "rest . . . on substantially similar policies and give rise to similar doctrines"); Robert R. Webb, *Privileges to Protect the Government*, 46 CHI.-KENT L. REV. 87, 92 (1969) (remarking that the state secret privilege and executive privilege are often confused "because the state secret privilege is usually invoked by an executive officer").

252. *See* El-Masri v. United States, 479 F.3d 296, 303 (4th Cir. 2007) (citing United States v. Nixon, 418 U.S. 683, 710–11 (1974)). The overlapping foundations in common law and constitutional law are not unique to the state secrets privilege. As courts and commentators have noted previously, to some extent all rules of federal common law perform a function of constitutional significance. *See* D.A. Jeremy Telman, *Our Very Privileged Executive: Why the Judiciary Can (and Should) Fix the State Secrets Privilege*, 80 TEMP. L. REV. 499, 506 (2007) (arguing that the privilege's origin is that it developed at common law, and that certain common law rules developed to protect "some essential constitutional core").

253. *Nixon*, 418 U.S. at 710–11.

Masri built on this dictum by alluding to the privilege's "function of constitutional significance," but it did not openly declare a constitutional basis.[254] Similarly, in *Egan*, the Court cited *Reynolds* and *Totten* in the context of the President's Article II authority to protect national security information.[255] However, executive privilege has more to do with the President's personal rights under the Constitution and less to do with the nature of the material at issue. The state secrets privilege, on the other hand, is precisely about the nature of the material at issue and its relationship with national security.[256] These broad propositions—all in dictum—that propose a broader constitutional privilege are counterbalanced by the Court's express characterization of the state secrets privilege in *Reynolds* and *General Dynamics Corp. v. United States*,[257] as well as the broader understanding of the privilege at the time Congress enacted FISA.[258]

FISA's *in camera*, *ex parte* procedures fit within a broader pattern of cooperation between Congress and the judiciary in policing executive action. Congress has the undisputed authority to promulgate and alter federal evidentiary rules, including by establishing procedures through which secret information can be disclosed either publicly or *in camera*.[259] The executive branch deserves deference on matters of national security and secrecy, but the executive's prerogative in this sphere remains subject to congressional action. While Judge Bumatay's dissent in *Fazaga* also relies on *Waterman*, the Court did not rely on any

---

254. *El-Masri*, 479 F.3d at 303; *see also* Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *23 (4th Cir. Sept. 15, 2021) (declining to resolve *El-Masri*'s lack of clarity).

255. *See* Dep't of Navy v. Egan, 484 U.S. 518, 527 (1988) (first citing United States v. Reynolds, 345 U.S. 1, 10 (1953); and then citing Totten v. United States, 92 U.S. 105, 106 (1876)).

256. *See* Zagel, *supra* note 89, at 892.

257. 563 U.S. 478 (2011).

258. *See Reynolds*, 345 U.S. at 10; *Gen. Dynamics Corp.*, 563 U.S. at 485. In its brief in *General Dynamics Corp.*, the United States noted the state secrets privilege's deep roots in the law of evidence and that the privilege "reflects the Executive's constitutional duty to protect 'military or diplomatic secrets[.]'" Brief for the United States at 23, *Gen. Dynamics Corp.*, 563 U.S. 478 (Nos. 09-1298 & 09-1302). However, the United States also conceded that Congress had attempted to regulate the privilege by statute, which underscores the common law evidentiary nature of the state secrets privilege. *See id.*

259. *See* Ronan E. Degnan, *The Law of Federal Evidence Reform*, 76 HARV. L. REV. 275, 277–78 (1962) (concluding that "congressional power over evidence in federal courts is plenary, restrained only by the federal constitution").

privilege in deciding the case.[260] However, Justice Jackson noted the Court's inability to sit *in camera* as one factor militating against judicial review of the Civil Aeronautics Board's order.[261] In FISA, however, Congress has explicitly authorized *in camera*, *ex parte* review to protect national security information.[262] Indeed, as Judge Motz noted in *Wikimedia*, courts have relied on such review when the government asserts that the state secrets privilege would preclude it from raising a valid defense to a constitutional claim.[263]

In doing so, FISA aligns more closely with other instances in which Congress has exercised its legislative power in collaboration with the judiciary to police executive action in areas of national security and secrets, such as through the Freedom of Information Act[264] (FOIA) and the Classified Information Procedures Act[265] (CIPA).[266] Congress, in drafting CIPA in particular, responded to concerns that criminal defendants would be able to force the government to reveal secret information, and the statute established special procedures governing the handling of such information, including during the discovery phase.[267] Similarly, FISA preserves the proper judicial role in preventing abusive executive power.[268]

---

260. *See* Chi. & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948).

261. *See id.* at 111.

262. 50 U.S.C. § 1806(f).

263. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *26 (4th Cir. Sept. 15, 2021). (Motz, J., concurring in part and dissenting in part) (collecting cases).

264. 5 U.S.C. § 552 (2018).

265. Pub. L. No. 96-456, 94 Stat. 2025 (1980) (codified as amended at 18 U.S.C. App. III).

266. *Cf.* Brief of Center for National Security Studies et al. as Amici Curiae Supporting Respondent at 19, United States v. Weatherhead, 528 U.S. 1042 (1999) (No. 98-1904) (arguing that FOIA, by making *in camera* judicial review available, did not present any of the constitutional issues raised in *Waterman*).

267. *See* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 207–08 (2010) (detailing the motivations behind CIPA's enactment); *see also* Fazaga v. FBI, 965 F.3d 1015, 1069 (9th Cir. 2020) (Gould & Berzon, JJ., concurring) ("The government uses these very same procedures all the time when prosecuting suspected terrorists; the government does so by choice, and without any evident handwringing over whether the use of the § 1806(f) procedures might lead to the disclosure of state secrets.") *cert. granted*, 2021 WL 2301971 (U.S. June 7, 2021) (No. 20-828).

268. The Supreme Court's grant of certiorari in two Ninth Circuit state secrets cases—*Fazaga* and *Zubaydah*—indicates that the Court may clarify the nature and scope of the privilege. The Supreme Court could agree with the Ninth Circuit in *Fazaga* and rule that FISA displaces the state secrets privilege. However, should the Court rule against the plaintiffs in *Fazaga*, it may opt to rule on statutory grounds, similar to the panel opinion in *Wikimedia*, by finding that Congress did not speak clearly enough to

2. Congress intended FISA to displace the state secrets privilege

Based on FISA's text, structure, and legislative history, Congress intended to displace the state secrets privilege in electronic surveillance cases. The Ninth Circuit correctly found that FISA speaks directly to the same issues underlying the federal common law state secrets privilege under *Reynolds*.[269] In enacting FISA, Congress explicitly acknowledged that the extant federal common law system had not only failed to properly balance national security and civil liberties, but also did not establish adequate safeguards against government abuse.[270] Therefore, in crafting FISA, Congress used broad and unequivocal language, echoing the Church Committee's recommendations to cover the field as it pertained to electronic

---

displace the privilege, assuming arguendo that the privilege is based in the common law and not the Constitution. Such a ruling would conform to the Court's constitutional avoidance doctrine and would in effect continue the Court's deferential posture toward the executive branch on national security matters. *See* Gomez v. United States, 490 U.S. 858, 864 (1989 ("It is our settled policy to avoid an interpretation of a federal statute that engenders constitutional issues if a reasonable alternative interpretation poses no constitutional question."); *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) ("[W]e have often found a lack of standing in cases in which the Judiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs[.]"). Should the Supreme Court take such an approach, Congress would remain free to regulate the privilege by statute.

However, a statutory ruling would not clarify much of the Court's murky state secrets analysis, and the Court may elect to set out a clearer and broader vision of executive power. Three justices from the majority in *Clapper*—Justices Alito, Thomas, and Roberts—remain on the Court, along with several newer justices with more expansive views of executive power. Justice Kavanaugh, in discussing *Nixon*, has characterized the state secrets privilege as an executive privilege. Brett M. Kavanaugh, *The President and the Independent Counsel*, 86 GEO. L.J. 2133, 2173 (1998). Justice Gorsuch, during his tenure with the Bush Administration, "participated in discussing litigation options" in *El-Masri*, and was commended for his work on the case after the Fourth Circuit dismissed the suit on state secrets grounds. *Confirmation Hearing on the Nomination of Hon. Neil M. Gorsuch to Be an Associate Justice of the Supreme Court of the United States: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 706 (2017) (statement of Jameel Jaffer). Should the Supreme Court rule that the state secrets privilege is constitutionally based, plaintiffs—and Congress—will need to rely on executive self-restraint, precisely the circumstance the Church Committee sought to avoid.

269. *Fazaga*, 965 F.3d at 1045. Both the Ninth Circuit and the Fourth Circuit analyzed FISA preemption under the "speak directly" standard, not under a clear statement standard as the government has argued. [CITE].

270. H.R. REP. NO. 95-1283, pt. 1, at 21 (1978).

surveillance.[271] The Fourth Circuit, in finding that § 1806(f) does not "speak directly" to the situation at issue in *Wikimedia*, relied on canons of statutory interpretation in cabining the meaning of § 1806(f) in a way that is inconsistent with FISA's plain text structure and purpose.

FISA's plain text—especially that of § 1806(f)—directly addresses the same circumstances as the state secrets privilege.[272] Both address the concern that civil litigation may force the government to reveal sensitive information, which, in the interest of national security, should not be revealed.[273] Both recognize that invocation of the privilege has serious ramifications for the pursuit of justice; therefore, courts must find a proper balance between national security, justice, and transparency.[274] Further, substantially similar circumstances trigger both the state secrets privilege and § 1806(f). In both cases, the government must invoke the privilege, and both § 1806(f) and the state secrets privilege foresee some individualized determination by the relevant head of a department.[275] Both § 1806(f) and the *Reynolds* privilege call on the court to review the invocation of the privilege without disclosing the underlying privileged information to determine how the suit should proceed.[276] Although the Supreme Court in

---

271. *See Fazaga*, 965 F.3d at 1072 (Gould & Berzon, JJ., concurring) (emphasizing that Congress used the broadest language possible).

272. *Fazaga*, 965 F.3d at 1046.

273. United States v. Reynolds, 345 U.S. 1, 10 (1953).

274. *See* Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1081 (9th Cir. 2010) (en banc) (emphasizing that courts must "[strike an appropriate balance] between protecting national security matters and preserving an open court system" (quoting Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1203 (9th Cir. 2007))).

275. *Compare id.* (requiring a sworn affidavit by the attorney general), *with Reynolds*, 345 U.S. at 7–8 (requiring a formal privilege lodged by the head of the relevant department). In *Wikimedia*, the Fourth Circuit sought to differentiate between the state secrets privilege as a shield (where it is invoked by the head of the department controlling the information) and FISA's § 1806(f) procedures as a sword (where it is invoked by the attorney general). Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *19 (4th Cir. Sept. 15, 2021). However, this difference is not material, especially under the Obama-era guidelines which require the Attorney General to approve the invocation of the privilege in order to defend it.

276. *Compare* 50 U.S.C. § 1806(f) (detailing the *in camera*, *ex parte* review process and emphasizing that disclosure to the aggrieved person, "under appropriate security procedures and protective orders," is only appropriate where "such disclosure is necessary to make an accurate determination of the legality of the surveillance"), *with Reynolds*, 345 U.S. at 8 ("The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect." (footnote omitted)).

Reynolds refrained from endorsing mandatory *in camera, ex parte* review, Congress was free to legislate a more stringent examination through FISA's § 1806(f) procedures. Therefore, by its own text, § 1806(f) creates an alternative mechanism to the state secrets privilege in electronic surveillance cases.

Further, Congress used broad and *mandatory* language to ensure FISA and other related surveillance statutes would be the exclusive means by which the government could conduct surveillance.[277] Congress was explicit that FISA's "exclusive means" clause "puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillance[] in the United States outside of the procedures contained in [FISA and Title III]".[278] The § 1806(f) procedures apply "notwithstanding any other law" and require courts to use the *in camera, ex parte* procedures "whenever" the Attorney General files an affidavit asserting that disclosure of particular evidence would create a risk to national security.[279]

FISA's legislative history further bolsters the reading of the statute as preempting the state secrets privilege in electronic surveillance cases. The Church Committee repeatedly emphasized the need to enact a "comprehensive legislative charter" on electronic surveillance.[280] The Church Committee's focus on a comprehensive piece of legislation was consistent with its key finding: without an adequate system of checks and balances, intelligence activities may run afoul of civil liberties.[281] The Church Committee also highlighted the role of the courts in

277. Jewel v. NSA, 965 F. Supp. 2d 1090, 1104–05 (N.D. Cal. 2013) (quoting the CHURCH COMMITTEE REPORT, *supra* note 23, at 296–97).

278. *See* S. REP. NO. 95-604, pt. 1, at 64 (1977); H.R. REP. NO. 95-1283, pt. 1, at 21 (1978). Notably, both the House and Senate made clear they considered "[w]hen the President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb." Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

279. 50 U.S.C. § 1806(f). In *Wikimedia*, because Judge Diaz found that Wikimedia's motion did not fulfill any of § 1806(f)'s three triggering conditions, it mentioned but did not rebut Wikimedia's assertion that the phrase "notwithstanding any other law" indicated Congress's intent to displace the privilege. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *19 (4th Cir. Sept. 15, 2021).

280. *See supra* Section I.B.1 (exploring the relationship between the Church Committee's key findings and recommendations).

281. CHURCH COMMITTEE REPORT, *supra* note 23, at 289. The Church Committee noted that "[m]ost domestic intelligence issues have not reached the courts, and in those cases when they have reached the courts, the judiciary has been reluctant to grapple with them." *Id.* at 6.

fostering a culture lacking in accountability and oversight. In enacting FISA, Congress recognized that the judiciary—by deciding cases without the benefit of reviewing all relevant material—had not balanced these interests in national security cases and instead had largely abdicated their role in ensuring executive accountability.[282] According to Congress, the judicial common law development of standards and restrictions governing electronic surveillance "threatens both civil liberties and the national security" because such development "occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court."[283]

The Church Committee also found that excessive executive power and secrecy represented another obstacle to effective oversight and accountability.[284] In particular, the Church Committee noted that at times this executive power was "seen as flowing not from the law, but as inherent in the Presidency," and that "[s]uch Executive power, not founded in law or checked by Congress or the courts, contained the seeds of abuse and its growth was to be expected."[285] Therefore, in crafting its recommendations for reform, the Church Committee emphasized that "[s]ecrecy should no longer be allowed to shield the existence of constitutional, legal and moral problems from the scrutiny of all three branches of government or from the American people themselves."[286]

Seen through this lens, FISA is not only a constraint on excessive executive power—it also embodies a repudiation of excessive judicial timidity when faced with matters of national security and electronic surveillance. Congress's intent to balance the need to properly protect national security information and the urgent need for judicial redress thus overlaps with the state secrets privilege.[287] Section 1806(f)'s

282. H.R. REP. NO. 95-1283, pt. 1, at 21 (1978).

283. *Id.* ("[T]he tiny window to this area which a particular case affords provides inadequate light by which judges may be relied upon to develop case law which adequately balances the rights of privacy and national security.").

284. *See* CHURCH COMMITTEE REPORT, *supra* note 23, at 292 (explaining how an expansive view of executive power, coupled with the secrecy of intelligence programs, had essentially insulated these programs from the normal system of checks and balances and shielded unlawful activity from scrutiny).

285. *Id.*

286. *Id.*

287. Judge Bumatay's dissent in *Fazaga* criticizes the court's reliance upon FISA's legislative history, emphasizing that courts have "no authority to enforce a principle" based on legislative history. Fazaga v. FBI, 965 F.3d 1015, 1081 (9th Cir. 2020)

procedures provide an avenue to judicial relief by requiring courts to check the executive branch's use of the state secrets privilege to stymie accountability.

3. Section 1806(f) applies to affirmative legal challenges to electronic surveillance

Congress intended § 1806(f)'s procedures to apply not only to cases where a criminal defendant seeks to obtain or suppress evidence derived from electronic surveillance, but also in affirmative civil challenges to the lawfulness of electronic surveillance.[288]

As the Ninth Circuit found in *Fazaga*, § 1806(f)'s *in camera* review procedures apply "whenever" an aggrieved person makes "any" motion or request "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."[289] By its plain text, this includes scenarios in civil litigation where an aggrieved person seeks to discover information derived from electronic surveillance, and the attorney general files an affidavit asserting a risk to national security.

In seeking to cabin this provision of § 1806(f) in *Wikimedia*, Judge Diaz relied on canons of statutory construction, at the expense of the actual text of the statute.[290] But such a narrow reading would also put § 1806(f) into conflict with other provisions of FISA—most notably, §

(Bumatay, J., dissenting) (quoting Shannon v. United States, 512 U.S. 573, 584 (1994)). However, notwithstanding criticism of the use of legislative history as a general proposition, there are a number of reasons why FISA's legislative history is uniquely suitable for analysis: (1) the FISC and Court of Review use legislative history in their published opinions; (2) FISA's legislative history is "unusually clear, univocal, and informative"; (3) national security law, unlike most other areas of law, concerns some matters that cannot be discussed openly; and (4) "because national security law depends so heavily on historical accommodations reached between the executive and legislative branches, legislative history provides a particularly important context in which to interpret statutory text." KRIS & WILSON, *supra* note 34, § 4:7; *see, e.g.*, *In re* Section 702 2020 Certification, slip op. at 29 (FISA Ct. Nov. 18, 2020) (relying on legislative history in support of its finding that Congress included § 1806(a) to make clear that government monitoring of privileged communications did not strip those communications of their privileged nature).

288. *See* H.R. REP. NO.95-1720, at 31 (1978) (Conf. Rep.).

289. 50 U.S.C. § 1806(f); *Fazaga*, 105 F.3d at 1050, 1053.

290. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *16–17 (4th Cir. Sept. 15, 2021).

1810—in violation of the whole-text canon.[291] Judge Diaz's opinion in *Wikimedia* downplays this "inconsistency" by emphasizing that "[e]very state secrets case presents the possibility that a plaintiff will be denied—in the interests of national security—a remedy available by law."[292] But, as the court in *Fazaga* noted, it would be counterintuitive for Congress to pass a comprehensive surveillance law, include in it a mechanism by which plaintiffs may sue to recover damages for unlawful surveillance, and incorporate procedures by which a court may determine the lawfulness of a given surveillance program, only to then refuse to make those procedures available for suits to recover damages.[293]

Indeed, FISA's legislative history buttresses a reading of the statute to extend to affirmative legal challenges. Both the House and Senate bills provided for civil and criminal actions arising out of unlawful surveillance.[294] While the House bill had bifurcated procedures for criminal and civil actions, the Senate bill utilized a single procedure for both types of claims.[295] In the end, the Senate mechanism—with some modification—prevailed, creating a single mechanism meant for both civil and criminal use.[296] In *Fazaga*, the Ninth Circuit rejected the government's contention that the § 1806(f) procedures only applied when the government initiates the legal action.[297] In *Wikimedia*, Judge Diaz agreed that § 1806(f) applies in both civil and criminal cases, but only when the *government* seeks to use the information.[298]

---

291. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 167–69 (2012) ("The text must be construed as a whole.").

292. *Wikimedia*, 2021 WL 4187840, at *20.

293. *Fazaga*, 965 F.3d at 1050–51. Nor is the use of § 1806(f)'s procedures limited only to suits brought under the civil remedy provision in § 1810. As *Fazaga* noted, the D.C. Circuit's decision in *ACLU Foundation* expressly endorsed the use of § 1806(f) for claims under FISA, as well as for claims of unconstitutional conduct. ACLU Found. of S. Cal. v. Barr, 952 F.2d 457, 465 (D.C. Cir. 1991) ("[T]he procedure mandated by § 1806(f) is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance.").

294. H.R. REP. NO. 95-1720, at 31.

295. *Id.*

296. *Id.* at 32.

297. *Fazaga*, 965 F.3d at 1049.

298. Wikimedia Found. v. NSA, No. 20-1191, 2021 WL 4187840, at *16 (4th Cir. Sept. 15, 2021). It appears the government also conceded in *Wikimedia* that § 1806(f)'s procedures apply regardless of who initiated the suit. *Id.*

Having found that FISA's § 1806(f) procedures displace the state secrets privilege in electronic surveillance cases, the remaining question is: who may properly access these procedures?

4. Section 1806(f)'s procedures apply even where the government seeks to shield evidence regarding whether a particular individual was subject to surveillance

In surveillance cases, such as *Jewel* and *Wikimedia*, plaintiffs face an additional barrier to pursuing their case—the government's invocation of the state secrets privilege to shield evidence establishing whether those plaintiffs were subject to surveillance, thereby making them "aggrieved persons" under FISA. The government and at least one district court have argued, however, that even assuming FISA displaces the state secrets privilege, plaintiffs may not invoke FISA's § 1806(f) procedures "where the very issue of standing implicates state secrets."[299] However, just as FISA's text, structure, and legislative history indicate that § 1806(f)'s procedures are available in affirmative challenges to surveillance programs, so too do they indicate the *in camera*, *ex parte* procedures' availability where the very issue of state secrets cuts to standing.

Under FISA, an "aggrieved person" is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[300] Following the government's argument, a plaintiff challenging a surveillance program must establish with certainty that they were subject to surveillance.[301] In the absence of discovery, plaintiffs would be left to rely on government notification of such surveillance—as the government has said it will do consistently in criminal trials—or on other official disclosures of information; however, depending on official government disclosures defeats the object and purpose of FISA's civil

299. *See* Jewel v. NSA, No. C 08–04373, 2019 WL 11504877, at *13 (N.D. Cal. Apr. 25, 2019) (distinguishing *Jewel* from *Fazaga* by finding that the unique procedural posture in *Jewel* did not foreclose the court from dismissing on state secrets grounds), *aff'd*, No. 19–16066, 2021 WL 3630222 (9th Cir. Aug. 17, 2021).

300. 50 U.S.C. § 1801(k).

301. *See, e.g.*, Brief for Appellees at 22, Jewel v. NSA, No. 19-16066, (9th Cir. Dec. 6, 2019) (arguing that establishing aggrieved person status is a threshold requirement to be determined prior to determination of the lawfulness of an electronic surveillance under § 1806(f)).

remedy.[302] Even in criminal cases, where the government has said it will give notice of FISA-derived evidence, it has not done so consistently.[303]

Both the Church Committee and FISA foresee courts' ability to fashion discovery procedures, including *in camera*, *ex parte* hearings, in order to allow plaintiffs with substantial claims to bring suit while protecting secret information. In outlining its vision for a civil remedy mechanism, the Church Committee emphasized that, while it believed that any citizen with a "substantial and specific claim to injury" arising from surveillance should have standing, it recognized "the need for judicial protection against legal claims which amount to harassment or distraction of government officials, disruption of legitimate investigations, and wasteful expenditure of government resources."[304] While the Church Committee recognized the risks associated with creating such a civil remedy, it believed that courts would be able to fashion discovery procedures, including *in camera* proceedings, to allow plaintiffs with "substantial claims" adequate discovery while protecting the secrecy of sensitive national security information.[305] FISA's language and legislative history again echo the recommendations of the Church Committee in creating such a procedure. In discussing FISA's "aggrieved person" status, the House noted that Congress intended the term to be "coextensive, but no

---

302. *See* Brief of Professor Stephen I. Vladeck as Amicus Curiae in Support of Appellant at 6, Wikimedia Found. v. NSA, No. 20-1191, (4th Cir. July 8, 2020) (emphasizing that forcing plaintiffs to prove their aggrieved status prior to unlocking § 1806(f) "turns Congress's carefully designed mechanism for ensuring a judicial check on surveillance abuses into an absurd Catch-22: only those able to prove that their communications were intercepted can use the provision; but only those who can use the provision are able to prove that their communications were intercepted"). This is also true of cases like *Fazaga* and *Al-Haramain* where the government provided—intentionally or not—notice and evidence of surveillance to the subjects of its surveillance programs.

303. *Id.* at 24–25 (noting that the government had not been providing notice to all criminal defendants against whom FISA surveillance was being used); Brief of Amici Curiae Americans for Prosperity Foundation et al. in Support of Plaintiff-Appellant and Reversal at 19–20, Wikimedia Found. v. NSA, No. 20-01191, at 19–20 (noting how the government had interpreted its FISA disclosure obligations narrowly).

304. CHURCH COMMITTEE REPORT, *supra* note 23, at 337, 338 n.70 (noting that this requirement "is intended to allow a judge to screen out frivolous claims where a plaintiff cannot allege specific facts which indicate that he was the target of illegal intelligence activity").

305. *Id.* at 337.

broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance."[306]

Adopting such a standard would not, as the government has posited, open the floodgates to plaintiffs challenging surveillance programs, including bad actors merely seeking to expose information about the underlying program.[307] The government's position echoes the Court's own fear of divulging sensitive national security information to adversaries, which would undermine the very purpose of such surveillance and harm national security. In *Clapper*, Justice Alito presented a hypothetical that echoes a major government concern regarding calls for greater disclosure.[308] In discussing the idea of an *in camera* proceeding to determine whether the government was in fact intercepting respondents' communications and what targeting or minimization procedures were used, Justice Alito posited that "this type of hypothetical disclosure proceeding 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."[309] In many ways, *Clapper* epitomizes federal courts' reluctance to address the merits of national security programs and the judicial tendency to rely on procedural obstacles to avoid doing so.[310] However, the *Clapper* hypothetical—which did not address

306. H.R. REP. NO. 95-1283, pt. 1, at 66. According to some commentators, the House report's text does not accurately describe the language Congress used in FISA. *See* KRIS & WILSON, *supra* note 34 § 29:5 (noting that in certain cases, an aggrieved person would not have standing because there was no reasonable expectation of privacy, or a person with standing would not have "aggrieved person" status where they had a reasonable expectation of privacy in a particular area but were not personally the target of or subjected to the surveillance).

307. *See, e.g.*, Brief for Appellees, *supra* note 301, at 23 (arguing that Jewel's interpretation of the "aggrieved person" standard would allow 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").

308. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 412 n.4 (2013).

309. *Id.* (noting that even if all protective procedures were successful, "the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets").

310. *See id.* at 409 ("[W]e have often found a lack of standing in cases in which the [j]udiciary has been requested to review actions of the political branches in the fields of intelligence gathering and foreign affairs."); *see also* Vladeck, *supra* note 10, at 1037 ("With a handful of narrowly circumscribed exceptions, courts faced with civil suits seeking remedies against allegedly unlawful government surveillance, detention, interrogation, rendition, and watch-listing, among myriad other initiatives, have refused to provide relief—and usually not because of a determination that the

specific *in camera, ex parte* proceedings such as those under § 1806(f)—is inapposite for several reasons.

First, under § 1806(f), a plaintiff challenging the lawfulness of a surveillance program must still allege their claims in sufficient detail and with sufficient facts to escape immediate dismissal.[311] In *Jewel*, the plaintiffs presented significant amounts of evidence, including: a declaration and documents from former AT&T technician Mark Klein; declarations from former NSA employees corroborating their claims; and documents published by media organizations.[312] Even Wikimedia, an organization that purportedly engages in more than one trillion international internet communications each year, has labored to establish its theory of standing, despite presenting significant amounts of evidence, including declassified FISC opinions, public disclosures from U.S. government officials, expert declarations, and leaked NSA documents.[313] Therefore, as a practical matter, the availability of § 1806(f) will continue to be a fact-intensive inquiry and may present insurmountable barriers to many plaintiffs.

Second, while there are concerns that the § 1806(f) procedure may force judges to disclose secret material to plaintiffs and their lawyers, there is no evidence that is the case. Under § 1806(f), the court may disclose all or part of the privileged information, taking into account appropriate protective measures, if it "is necessary to make an accurate determination of the legality of the surveillance."[314] However, far from mandating any disclosure of information, FISA appears to frame disclosure to the plaintiffs or their attorneys as a measure of last resort,

---

underlying government conduct was lawful, but rather because of obstacles that, in the courts' views, barred them from even reaching the merits of the plaintiffs' claims." (footnote omitted)).

311. *See* Fazaga v. FBI, 965 F.3d 1015, 1053 (9th Cir. 2020) (explaining that the plaintiffs were aggrieved persons because they had a reasonable expectation of privacy).

312. *See* Jewel v. NSA, No. C 08-04373, 2019 WL 11504877, at *7–10 (N.D. Cal. Apr. 25, 2019) (evaluating the plaintiffs' evidentiary proffer).

313. *See* Brief for Plaintiff-Appellant, *supra* note 203, at 7–8 (arguing that Wikimedia had standing based on the number of international internet connections and the government's interception and retention of communications between foreign users and Wikimedia's U.S.-based servers and communications between U.S. users and Wikimedia's foreign servers).

314. 50 U.S.C. § 1806(f).

and courts that have used *in camera, ex parte* procedures have uniformly refused to reveal any privileged information.[315]

Finally, as the district court found in *Jewel*, there may be situations in which—after conducting its *in camera, ex parte* review—the court still must dismiss the case on state secrets grounds. In *Jewel*, the district court reviewed *in camera* and *ex parte* classified government declarations regarding the alleged surveillance programs.[316] After reviewing the materials, the district court issued a short order dismissing the case on state secrets grounds, as well as a classified opinion reviewing the classified submissions and its reasoning for dismissal.[317] The court emphasized that it owed great deference to the executive branch's claim 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," echoing the Supreme Court in *Clapper*.[318] Conducting *in camera, ex parte* review under § 1806(f) ensures that the court is properly vetting the Executive branch's claim of privilege prior to resorting to the extreme option of dismissing a case. In failing to doing so, as the Fourth Circuit did in *Wikimedia*, courts are endorsing precisely the extreme deference to the executive branch that FISA sought to end.

Jewel does not foreclose the possibility that, given existing public knowledge about the broad parameters of these surveillance programs and the lack of individualized targeting for collection, a similar procedure—by which a court may file a short public order granting or denying relief accompanied by a classified opinion—would not reveal significant information beyond what is already in the public sphere. Unlike the plaintiffs in *Clapper* who claimed their communications had been collected because they were in contact with individuals *targeted* by NSA surveillance,[319] the plaintiffs in *Jewel* and *Wikimedia* do not allege

315. *See* Fazaga v. FBI, 965 F.3d 1015, 1069 n.1 (9th Cir. 2020) (Gould & Berzon, JJ., concurring) ("As far as we are aware, there has *never* been a disclosure under FISA.").

316. Jewel v. NSA, No. C 08-04373, 2019 WL 11504877, at *13 (N.D. Cal. Apr. 25, 2019) (emphasizing that its comprehensive review of the classified material "distinguishes this case from *Fazaga*, and in fact from any other case involving state secrets cited by the parties or known to this Court").

317. *Id.* at *13–14 (finding that permitting further proceedings would jeopardize the national security).

318. *Id.* at *13; *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 412 n.4 (2013) (describing a hypothetical where allowing a standing inquiry to be settled by an *in camera* proceeding would undermine national security because any post-disclosure decision would alert the terrorist to whether their name was on a watch list).

319. *Clapper*, 568 U.S. at 407.

that the government targeted them for surveillance, but merely that it had incidentally collected their communications.[320] Further, as the district court in *Jewel* found, the plaintiffs there had much stronger allegations of standing than the plaintiffs in *Clapper* because they alleged past incidents of actual government interceptions of their electronic communications, as opposed to anticipated future interceptions.[321]

Having analyzed the relationship between FISA and the state secrets privilege, Congress clearly intended FISA to displace the privilege in electronic surveillance cases. While the Ninth Circuit in *Fazaga* did not address NSA surveillance programs, its analysis persuasively indicates the availability of § 1806(f)'s procedures in cases like *Jewel* and *Wikimedia*, where the government's invocation of the privilege covers evidence relating to whether the plaintiff was subject to surveillance, thus making them an "aggrieved person" under FISA. The availability of § 1806(f) as a mechanism for individual redress has important implications for U.S. national security policy and the United States' relationships with key allies in Europe.

III. WHY REDRESS MATTERS

The intelligence community must maintain the trust of the American public and foreign partners in order to effectively carry out its mission.[322] A growing number of countries have recognized that ensuring the availability of redress for harm resulting from unlawful national security actions does not undercut the effectiveness of those programs.[323] Providing viable pathways for redress signals that the civil

320. Jewel v. NSA, 673 F.3d 902, 906 (9th Cir. 2011); Wikimedia Found. v. NSA, 427 F. Supp. 3d 582, 588 (D. Md. 2018); *see supra* note 71 (explaining the concept of incidental collection).

321. *Jewel*, 673 F.3d at 910–11.

322. *See* OFF. OF THE DIR. OF NAT'L INTELLIGENCE, NATIONAL INTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA 24 (2019) (emphasizing that adhering to core principles of protecting privacy and civil liberties is integral to earn and retain public trust in the intelligence community, which in turn "directly impacts [intelligence community] authorities, capabilities, and resources").

323. *See* Brief of Center for Democracy & Technology and New America's Open Technology Institute as Amici Curiae in Support of Plaintiff-Appellant at 8–19, Wikimedia Found. v. NSA, No. 20-1191 (4th Cir. July 8, 2020) (examining European countries' discussion of surveillance capabilities in litigation over bulk collection programs).

liberties at the heart of American society cannot be "sacrificed at the altar of national security."[324]

Redress for unlawful surveillance implicates the United States' international relationships—both security-based and economic—and has important ramifications in both the public and private sectors.[325] In particular, the existence of meaningful avenues for judicial redress for unlawful surveillance cuts to the viability of important data-sharing agreements with the European Union, such as the E.U.-U.S. Privacy Shield.

A. Importance of Redress for E.U.-U.S. Data Sharing

The issue of individual remedies will likely continue to plague ongoing data-sharing efforts between the United States and European Union. The CJEU struck down the E.U.-U.S. Privacy Shield in part due to the lack of actionable rights in U.S. courts.[326] While the U.S. government has contended that the CJEU overlooked paths for attaining individual redress for violations of FISA section 702, its assertions that FISA does not preempt the state secrets privilege elucidates the tension between these positions.[327]

Prior to the *Schrems II* decision, the United States created a Privacy Shield Ombudsperson at the U.S. Department of State to allay the CJEU's concerns about oversight and redress.[328] Under this framework, the Ombudsperson would act as a point of contact for foreign governments with concerns over U.S. surveillance activities.[329] Further, in the event of non-compliance, the Ombudsperson, in cooperation with "other oversight compliance review mechanisms," had the authority to provide foreign governments with "positive" responses—namely that any non-compliance had been remedied.[330]

---

324. Barack Obama, Remarks by the President on Review of Signals Intelligence, (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [https://perma.cc/84MK-9B5Y]; *see* Sinnar, Procedural Experimentation and National Security in the Courts at 1042.

325. *See* Obama, *supra* note 324 ("[J]ust as we balance security and privacy at home, our global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and leaders around the world.").

326. *See supra* Section I.B.3 (discussing the *Schrems II* decision).

327. *See supra* Section I.B.3; *see also* Brief for Appellees, *supra* note 301, at 30–31.

328. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 43 (July 16, 2020).

329. *Id.* ¶ 45.

330. *Id.*

In *Schrems II*, however, the CJEU rejected the Ombudsperson redress system as inadequate for two primary reasons: first, the Ombudsperson was not seen as sufficiently independent of the executive branch, and second, its decisions were not binding on intelligence agencies themselves.[331] Therefore, the CJEU found that the Ombudsperson mechanism did not comply with Article 47 of the European Charter, which provides for a hearing "before an independent and impartial court."[332]

In the wake of *Schrems II*, experts have suggested a number of alternative redress mechanisms that may meet the CJEU's standards. Notable alternatives include administrative grievance mechanisms with judicial review, either by a more robust version of the Privacy and Civil Liberties Oversight Board (PCLOB) or an expanded FISC.[333]

The PCLOB is an attractive venue for review given its reputation for independence (at least within the confines of the executive branch) and its positive reputation in Europe.[334] However, crafting an independent and impartial redress mechanism out of the PCLOB would require a significant overhaul for several reasons.[335] First, despite its important role in offering oversight and advice, the PCLOB's recommendations are non-binding.[336] Therefore, short of significantly expanding the PCLOB's power to approximate that of a court, any avenue for review by the PCLOB would have to be appealable to an Article III court. Second, as currently constituted, the PCLOB only has jurisdiction over information collected and used for anti-terrorism purposes.[337] Therefore, Congress would need to expand the PCLOB's

---

331. Kenneth Propp & Peter Swire, *After* Schrems II*: A Proposal to Meet the Individual Redress Challenge*, LAWFARE (Aug. 13, 2020, 7:28 PM), https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge [https://perma.cc/2JZQ-REAN]; *see* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶¶ 195–96 (July 16, 2020) (noting that the Ombudsperson was subject to dismissal by the Secretary of State and that there was no indication the Ombudsperson had power to adopt decisions binding on intelligence agencies).

332. *Schrems II*, ¶¶ 194.

333. *See* Propp & Swire, *supra* note 331 (discussing the fitness of both the PCLOB and FISC as potential factfinders in redress proceedings).

334. *Id.*

335. *Id.*

336. Setty, *supra* note 10, at 101.

337. RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD 196 (2013) (noting that this limited jurisdiction creates temptations for intelligence agencies to "mischaracterize their activities as something other than anti-terrorism" to avoid PCLOB review).

jurisdiction or replace it with a board with greater agency—as recommended by the President's Review Group on Intelligence and Communications Technologies in 2013.[338] Finally, the PCLOB's structural flaws—including long periods without the quorum it needs to advise and publish reports—hamper consistent independent oversight.[339] Therefore, any reform bolstering the PCLOB's role as a fact-finder would require more robust protections and staffing resources. However, even with greater reforms, the PCLOB remains part of the Executive branch, which may prove fatal.

The FISC is also a particularly attractive alternative given the court's experience examining surveillance programs while protecting sensitive information.[340] Further, despite continued criticism, Congress has instituted a number of FISC reforms, including the introduction of expert amici.[341] However, the FISC—like the PCLOB—would also require further reform to create a meaningful mechanism for redress.

By contrast, traditional Article III courts are already well positioned to act as factfinders in these cases. Further, as FOIA and CIPA demonstrate, district courts have experience evaluating national security information and establishing procedures to balance national security with the vindication of rights.[342]

B. Potential Legislative Solutions

As experts have noted, the current state of transatlantic data transfers is not sustainable.[343] However, the United States appears to be at an impasse in negotiations over replacing the defunct Privacy Shield

---

338. *Id.* (recommending the creation of a new independent agency known as the Civil Liberties and Privacy Protection Board).

339. Tonya Riley, *Civil Liberties Groups Pressure White House to Fill Surveillance Oversight Board*, CYBERSCOOP (Sept. 10, 2021), https://www.cyberscoop.com/privacy-pclob-biden-black-lives-matter [https://perma.cc/4G9K-X6VA]; Steven Katz, *The Executive Branch Needs Intelligence Oversight Reform*, JUST SEC. (Sept. 16, 2021), https://www.justsecurity.org/78245/the-executive-branch-needs-intelligence-oversight-reform [https://perma.cc/CU74-NE2R].

340. *See* Propp & Swire, *supra* note 331 (arguing that the FISC is better suited than traditional Article III courts).

341. *See* 50 U.S.C. § 1803(i) (codifying the amicus curiae provisions).

342. *See supra* note 120 (detailing FOIA and CIPA procedures).

343. *See* Julian Sanchez, *TikTok,* Schrems II*, and Cross-Border Data Flows*, CATO INST. (July 6, 2021), https://www.cato.org/blog/tiktok-schrems-ii-cross-border-data-flows [https://perma.cc/8ZAK-A8GS] (noting that the European Union's updated "Standard Contractual Clauses" will place a significant burden on companies).

framework.[344] According to reports, E.U. officials believe that "[t]o make the pact stick . . . the U.S. must make legislative changes to limit how American national security agencies can access European data, and give EU citizens a more meaningful way to challenge that access in U.S. courts."[345] Therefore, Congress should take advantage of the current swell of support for privacy legislation to reaffirm the availability of redress for surveillance harms.

As others have suggested, these reforms should include the codification of Presidential Policy Directive 28 and other protections for non-U.S. persons.[346] Along with codifying these rights, Congress should also renew its efforts to remove impediments to redress, including by regulating the state secrets privilege.[347] As an initial effort, Congress could reintroduce the State Secrets Protection Act, which would provide a framework for both the invocation and assessment of privilege claims.[348]

Should Congress be unable to consolidate support for broader regulation of the state secrets privilege, it could take a narrower path by passing legislation merely reaffirming Congress's intent to have FISA displace the privilege in electronic surveillance cases. The narrower approach comes with costs, including the failure to provide relief for individuals harmed by other national security programs, such as the CIA's extraordinary rendition program. Nonetheless, a narrower piece of legislation reaffirming Congress's intent for FISA to preempt the state secrets privilege would strengthen avenues for surveillance redress at a time when there may be greater bipartisan support for FISA reform.

---

344. See Vincent Manancourt & Mark Scott, *Washington Says a Transatlantic Data Deal Is Close. Brussels Disagrees.*, POLITICO (Sept. 17, 2021, 6:30 AM), https://www.politico.eu/article/washington-transatlantic-data-deal-brussels [https://perma.cc/P62Y-6BKA] (noting that the United States and European Union had failed to find a breakthrough in negotiations as of September 2021, in part because E.U. officials are "keen to avoid the ignominy of having a third data transfer deal struck down by [the CJEU]").

345. *Id.*

346. *See* Ira Rubenstein & Peter Marguiles, *Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground*, CONN. L. REV. (forthcoming) (manuscript at 48).

347. *See supra* Section I.C.2 (discussing prior attempts to regulate the privilege by statute).

348. *See supra* Section I.C.2.

CONCLUSION

The Ninth Circuit in *Fazaga* correctly recognized that FISA's § 1806(f) procedures displace the state secrets privilege in electronic surveillance cases and provide a mechanism through which courts may balance the government's need for secrecy with plaintiffs' right to challenge the lawfulness of surveillance programs. While the government has argued that the state secrets privilege is a constitutional rule rooted in the separation of powers, the Supreme Court in *Reynolds* and its progeny emphasized the common law evidentiary nature of the rule, leaving it open for congressional regulation. FISA's text, legislative history, and purpose indicate Congress's intent to displace the state secrets privilege, even where the government seeks to invoke the privilege to shield information relating to whether or not a particular plaintiff was subject to surveillance.

While FISA procedures remain secretive and deferential to the government, they offer an important opportunity for redress. By using § 1806(f)'s procedures, plaintiffs have greater actionable rights in U.S. courts, which may bring the United States into greater alignment with Europe on data protection and redress for surveillance abuses. Most importantly, FISA's procedures recognize that "the fundamental principles of liberty include devising means of forwarding accountability while assuring national security."[349] The government's continued use of the state secrets privilege to insulate surveillance programs from judicial review shows that, despite the executive branch's efforts to self-regulate its invocation of the privilege, a renewed discussion in Congress on its oversight role in this context is needed.

349. Fazaga v. FBI, 965 F.3d 1015, 1068 (9th Cir. 2020), *cert. granted*, No. 20-828, 2021 WL 2301971 (June 7, 2021).