2024

Picture This: In Camera Review of State Secrets Doctrine Claims Under FISA Section 702

Nicholas E. Pollera

PICTURE THIS: *IN CAMERA* REVIEW OF STATE SECRETS DOCTRINE CLAIMS UNDER FISA SECTION 702

Nicholas E. Pollera*

I. INTRODUCTION

Government surveillance in the post-9/11 era has been far reaching. Following the 9/11 terrorist attacks, the intelligence community's surveillance capabilities were expanded dramatically as a result of statutory changes to the Foreign Intelligence Surveillance Act (FISA).[1] These changes opened the floodgates for signals intelligence collection. In 2021 alone, United States intelligence agencies targeted over two hundred thousand non-U.S. persons under Section 702 of FISA.[2] Even more worrisome, under Section 702, the Federal Bureau of Investigation (FBI) alone queried over 3.3 million United States persons that same year.[3] Specifically, Section 702 has enabled surveillance of targets without an individual court order, even if a United States citizen's information gets collected during the surveillance.[4] Perhaps unsurprisingly, in parallel to this increase in surveillance is an increase in the government's use of state secrets privilege to effectively stop civil litigation when challenged for improper surveillance.[5] Furthermore, the federal courts' interpretation of the state secrets doctrine and 50 U.S.C. § 1806(f) has had a limiting effect on how aggrieved persons can effectively challenge the legality of government surveillance

* J.D. Candidate, 2024, Seton Hall University School of Law, B.A; Political Science, 2012, Gettysburg College. I wish to thank Professor Jonathan Hafetz for sharing his advice and knowledge on this topic, as well as Rachel Leung for her guidance throughout the writing process. Special thanks to my friend and colleague Alex Pilla for helping me come up with a clever title for this comment.

[1] Walter F. Mondale et al., *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2263 (2016).

[2] OFF. OF C. L. PRIVACY AND TRANSPARENCY, ANNUAL STATISTICAL TRANSPARENCY REPORT, REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2021, at 4 (Apr. 2022).

[3] *Id.*

[4] Mondale, *supra* note 1, at 2263; 122 Stat. 2436, Pub. L. 110-261, Sec. 702(a) (codified at 50 U.S.C. § 1881(a)).

[5] Margaret B. Kwoka, *The Procedural Exceptionalism of National Security Secrecy*, 97 B.U. L. REV. 103, 118 (2017); Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931, 1939 (2007).

for civil liberty violations. There are many significant legal concerns pertaining to the current surveillance apparatus, including barriers to a plaintiff establishing standing, Fourth Amendment concerns, and privacy problems, all of which are mostly outside the scope of this Comment. While I will provide a background survey of the legal framework of intelligence surveillance, this Comment will focus on the means by which aggrieved persons may challenge the legality of surveillance when the government invokes state secrets privilege. Specifically, I will argue that Congress should amend FISA § 1806(f) to require *in camera* review when the state secrets privilege is invoked.

In order to provide a framework by which plaintiffs may more effectively challenge United States intelligence agencies' use of surveillance, Congress should amend 50 U.S.C. § 1806(f) as follows. When a party brings suit for unlawful surveillance, and the government invokes state secrets privilege, before accepting the governments assertion trial courts should be required to review the confidential information *in camera* to determine whether disclosure or continued litigation would truly pose a national security risk. Part II of this Comment will provide a background on the surveillance abuses of the 20th century that led to the formation of the Church Committee and the reforms which came from the Committee's recommendations, including the Foreign Intelligence Surveillance Act of 1978 and the Foreign Intelligence Surveillance Courts. I will also cover how the modern state secrets doctrine came to be, and how it has been applied in two recent cases where plaintiffs have invoked § 1806(f). Part III will provide an analysis of why there should be a statutory amendment to § 1806(f), explicitly requiring district court judges to review, *in camera*, information over which the government is invoking state secrets privilege when FISA is considered for renewal in 2023. I will argue that the Executive branch's recent attempts to expand the interpretation of state secrets doctrine to one which acts as a justiciability bar is

misguided. I will also argue that that the federal judiciary is well prepared to take on the role of determining whether confidential information may be used in litigation and preventing disclosure. State secrets privilege should not act as an automatic trump card for the government simply because it was developed to protect our nation from legitimate national security risks. It should not protect the federal government from accountability.

II. BACKGROUND

A. *Prior to the Foreign Intelligence Surveillance Act*

Section A will discuss the surveillance case law leading up to the Church Committee, and the Committee itself, which addressed surveillance oversteps by the United States government. The findings and recommendations put forward by the Church Committee would lead to passage of the Foreign Intelligence Surveillance Act.

1. Katz and Keith

The *Katz* and *Keith* holdings highlight how the Supreme Court's view on surveillance during a period of surveillance excesses. In *Katz v. United States*, the petitioner was convicted of transmitting wagering information by telephone, after FBI agents had, without a warrant, attached an electronic recording device to the outside of a public telephone booth.[6] On appeal, the Ninth Circuit Court rejected the petitioner's argument that his Fourth Amendment rights were violated because "there was no physical entrance into the [phonebooth]." The Supreme Court, however, ruled that the FBI's warrantless electronic surveillance "violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure'" within the meaning of the Fourth Amendment.[7]

[6] 389 U.S. 347, 348 (1967).
[7] *Id.* at 353.

But the *Katz* majority opinion did not consider warrantless searches in a national security context. In his concurring opinion, Justice Douglas warned that any distinction of afforded protection based on the type of crime would be unconstitutional.[8] Further, a distinction for national security concerns would give the Executive Branch a "green light" to label matters as national security concerns to skirt warrant requirements.[9] Justice Douglas argued that the Executive is not, nor should it be, especially in cases of national security, a "detached, disinterested, and neutral" party.[10] Therefore, a neutral and disinterested magistrate is needed to the evaluate the validity of proposed searches when national security is involved.[11]

Almost five years later, the Court would revisit the question of warrantless searches and national security in *United States v. United States District Court for the Eastern District of Michigan* ("*Keith*"). There, the Court considered whether the Executive had the power to authorize electronic surveillance in domestic security matters without a judge-approved warrant.[12] The Court employed the reasoning of Justice Douglas' concurrence in *Katz*, that those with "investigative and prosecutorial dut[ies] should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks," and that "unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[13] The Court also noted that "[j]udges may be counted upon to be especially conscious of security requirements in national security cases."[14] While this case was dealt with the approval of warrants, note that the Court recognized the judiciary's ability to deal with sensitive information in a national security context. Ultimately, the Court held that

[8] *Id.* at 360.
[9] *Id.* at 359.
[10] *Id.* at 359–60.
[11] *Id.*
[12] 407 U.S. 297, 299 (1972).
[13] *Id.* at 317.
[14] *Id.* at 321.

prior judicial approval of a warrant is required in the case of domestic national security cases but expressed no opinion on surveillance of foreign powers.[15]

Once again, Justice Douglas offered a concurring opinion, this time calling out a distinction for Fourth Amendment concerns regarding electronic surveillance. While traditional Fourth amendment concerns, such as a search incident to an arrest, have been deterred by the potential damages actions against police, bad publicity, and reform, such "safeguards" are not available or ineffective when a victim is unaware that their Fourth Amendment rights have been violated.[16] With such safeguards potentially diminished, it is especially important that victims do not also lose their ability to seek redress through the Courts. Ultimately, the decisions in *Katz* and *Keith* did not put a stop to government overreach, and legislative reform was needed.

2. The Church Committee, the Foreign Intelligence Surveillance Act, and its Subsequent Amendments

In January of 1975, because of allegations of substantial wrongdoing, the United States Senate established a committee to investigate potential illegal or improper activities by the intelligence community.[17] The wrongdoing included illegal and improper covert actions, mail opening, monitoring and electronic surveillance of citizens, and political abuse.[18] To summarize the issues, "[t]oo many people have been spied upon by too many Government agencies and to [sic] much information has beeen [sic] collected."[19] This committee, known as the Church Committee after its chairman Senator Frank Church, published its findings in a report titled Intelligence Activities and the Rights of Americans.[20] The Committee was instructed to determine,

[15] *Id.* at 321–22.
[16] *Id.* at 324–25.
[17] SEN. REP. NO. 94-755, Book II, at V (1976) [hereinafter *Church Committee Report*].
[18] *Id.* at 5–13.
[19] *Id.* at 5.
[20] *Id.* at I–II.

amongst other mandates, whether existing laws were inadequate to protect the rights of United States citizens, and to improve executive and legislative control of intelligence activities.[21] There were three major questions the Committee endeavored to answer: (1) whether domestic intelligence activities were consistent with law and Constitutional rights, (2) whether foreign intelligence activities served the national interest, and (3) whether institutional procedures adequately ensured the intelligence community's compliance with law and the constitutional system of checks and balances.[22] The Committee acknowledged that their task was one of balance between crucial national security concerns, in which the intelligence community performs "necessary and proper" functions, and those of individual liberty and justice.[23] The central goals of the Committee were to make recommendations about which intelligence activities should be permitted, restricted, or prohibited, and what controls or organizational reforms should to be put in place to ensure intelligence operations are effective and in line with the country's values and interests. [24]

Examining cases beginning with Franklin D. Roosevelt's presidency through the Nixon administration, the Committee concluded that "intelligence excesses . . . have been found in every administration."[25] They found that privacy and free speech rights had been violated through the intelligence community's excessive surveillance activities, and among the many recommendations to come out the Committee's report was that civil remedies be available for those that have a suffered a harm from improper surveillance and that those with a "substantial and specific claim to injury" should have standing to sue.[26] But, the Committee also recognized that any scheme to

[21] *Id.* at VI.
[22] *Id.* at VI–VII.
[23] *Church Committee Report* at VII.
[24] *Id.* at IX.
[25] *Id.* at VIII; Mondale et al., *supra* note 1, at 2253 n.8.
[26] *Church Committee Report* at 336–37.

enable civil remedies needed to be balanced with national security interests, by allowing intelligence agencies to operate without being restricted from performing proper intelligence activities.[27] The Committee trusted that, in litigation, the judiciary would be able to balance the interests of a plaintiff's liberties with that of the government's national security concerns:[28]

> [W]e believe that the courts will be able to fashion discovery procedures, including inspection of material in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest.[29]

The Church Committee saw the importance of creating a legislative scheme whereby those with legitimate claims for illegal surveillance would have a statutorily provided avenue for bringing those claims against the government, even when the subject of those claims dealt with sensitive national security subjects.

B. *The Foreign Intelligence Surveillance Act and its Subsequent Amendments*

Section B will explore the development of the Foreign Intelligence Surveillance Act and the United States government's use of its statutory authority to carry out surveillance programs. This section will also explore disclosures of intelligence agency surveillance programs and subsequent amendments made to FISA as a result.

1. The original Foreign Intelligence Surveillance Act

As a result of the Church Committee's findings, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) and created the Senate and House Select Committees on Intelligence to provide oversight of the United States intelligence agencies.[30] FISA and the

[27] *Id.* at 336.
[28] *See Id.* at 337.
[29] *Id.* at 337.
[30] Pub. L. No. 950511, 92 Stat, 1783 (codified as amended at 50 U.S.C. § 1801 (1978)); S. Res. 400, 94th Cong. (1976); H.R. Res. 591, 94th Cong. (1976).

Congressional oversight committees were "meant to provide a more concrete legal framework capable of limiting and guiding intelligence agencies."[31] The Act included § 1806(f), which appears to provide a method for review of potentially confidential surveillance information when challenging the legality of surveillance.[32] § 1806(f), titled "In camera and ex parte review by district court," reads as follows:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.[33]

50 U.S.C. § 1806(k) defines an "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[34]

FISA also established the Foreign Intelligence Surveillance Courts (FISC or FISA Courts), which "have jurisdiction to hear applications for and grant orders approving electronic

---

[31] Mondale et al., *supra* note 1, at 2262.
[32] *See* 50 U.S.C. § 1806(f).
[33] § 1806(f). Black's Law Dictionary defines "In Camera" as "In the judge's private chambers" or "[i]n the courtroom with all spectators excluded." *In Camera*, BLACK'S LAW DICTIONARY (11th ed. 2019). It defines the term "Ex Parte" as "[d]one or made at the instance and for the benefit of one party only, and without notice to, or argument by, anyone having an adverse interest; or relating to, or involving court action taken or received by one party without notice to the other . . ." *Ex Parte*, BLACK'S LAW DICTIONARY (11th ed. 2019).
[34] *Id.* at § 1801(k).

surveillance[.]"[35] Following the Church Committee and enactment of FISA and the FISC up until 2001, the government mostly adhered to the Committee's recommended model, following three key components: (1) the only approved applications were individualized warrants submitted for approval to the FISC court prior to the search occurring, (2) the only approved warrants were those for the "gathering of intelligence information from 'foreign power[s]' or 'agents of foreign power[s],'" and (3) "if the information requested was related to or concerned a United States person [it] had to be 'necessary' to obtaining foreign intelligence information."[36]

2. The PATRIOT Act

In the wake of the September 11 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act).[37] The Act was passed quickly as an emergency-response measure without the amount of debate expected for such significant legislation.[38] The PATRIOT Act represented a significant departure from the original FISA framework, greatly expanding what was subject to FISC warrants.[39] For example, whereas previously the government needed to provide "specific and articulable facts" that a business records request from a common carrier pertained to a "foreign power or agent or a foreign power,"[40] the FBI could now request a FISC order for "the production of any tangible thing" from any business "so long as there were reasonable grounds to believe it was 'relevant' to an authorized investigation."[41]

---

[35] *Id.* at § 1803(a); *see also* Pub. L. No. 95-511, Sec. 103(a), 92 Stat. 1783 (the original act or Congress).
[36] Mondale et al., *supra* note 1, at 2262–63, (quoting Foreign Intelligence Surveillance Act of 1978 §§ 101(e)(1)(A) and 101(e)(1)) (brackets in original).
[37] Pub. L. No. 107–56, 115 Stat, 272.
[38] Elizabeth Goitein & Faiza Patel, *What Went Wrong With the Fisa Court*, BRENNAN CTR. FOR JUST., 22 (2015); s*ee also* Pub. L. No. 107-56, 115 Stat, 272 (the PATRIOT Act was went into effect on October 26, 2001, just forty-five days after the September 11th terrorist attacks).
[39] Mondale et al., *supra* note 1, at 2264.
[40] *Id.* at 2264.
[41] *Id.*

What ultimately took place as a result of the post-9/11 era FISA amendments was a change in standards by which the FISA Courts evaluated surveillance order requests.[42] Where previously the government was required to certify that "the purpose" of the surveillance was to acquire foreign intelligence, the government only had to certify that "a significant purpose" of the surveillance activity was to acquire foreign intelligence under the PATRIOT Act.[43] The original standard was a requirement to ensure that the government did not pretextually use foreign intelligence or national security to carry out domestic surveillance without a warrant.[44]

3. The FISA Amendments Act of 2008

Another significant change, and perhaps the most significant change for the purposes of this Comment, was the FISA Amendments Act of 2008 (FAA).[45] The FISA of 1978 had required probable cause that the government's surveillance target was a "foreign power or agent of a foreign power," but this requirement was removed for programmatic surveillance by the FAA.[46] The FAA included Section 702, which provides for "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[47] While Section 702 did include some limitations, such as prohibiting intentional targeting of persons known to be in the U.S. or U.S. persons abroad,[48] these restrictions were not enough to prevent intelligence agencies from implementing large-scale, wide-reach surveillance programs such as Upstream and PRISM,[49] which will be discussed further in the following sub-sections. The FAA ushered in these programmatic surveillance programs by eliminating the need for individual court orders for

[42] *Id.* at 2265; Goitein & Patel, *supra* note 38, at 22.
[43] Goitein & Patel, *supra* note 38, at 23.
[44] *Id.*
[45] *See* 122 Stat. 2436, Pub. L. 110-261.
[46] Goitein & Patel, *supra* note 38, at 41.
[47] 122 Stat. 2436, Pub. L. 110-261, Sec. 702(a) (codified at 50 U.S.C. § 1881(a)).
[48] *Id.* at §§ 702(b)(1), (2), and (3).
[49] OPEN TECH. INST., *Section 702's Excessive Scope Yields Mass Surveillance: Foreign Intelligence Information, PRISM, and Upstream Collection*.

surveillance programs, even when a U.S. citizen's information may be collected as part of the surveillance, as long as that citizen was not the target.[50] This represented a significant departure from the original tenets of the Church Committee. Whereas the original FISA required the FISC to make individual determinations as to whether a surveillance warrant would be approved, the FAA "transformed the FISC into a meta-arbiter, approving generally applicable targeting and minimization procedures that applied after a search occurred."[51]

4. Snowden Disclosures and the FREEDOM Act

In June of 2013, a National Security Agency (NSA) contractor and former CIA employee named Edward Snowden, released information about NSA surveillance through the American and British press.[52] The first of these reports detailed a FISA court order requiring Verizon to hand telephony data to the NSA.[53] The classified order required Verizon and its subsidiaries to turnover all call detail records for communications between the United States and outside the country, and those within the United States, created by Verizon.[54] The following day the press released details of another United States surveillance program whereby the NSA and FBI were gathering information from servers of United States internet companies.[55] This program, codenamed

[50] *See* Mondale et al, *supra* note 1, at 2266–67. *See also* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 35 (2014).
[51] Mondale et al., *supra* note 1, at 2266–67.
[52] Glenn Greenwald, Ewen MacAskill, and Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM) https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald and Ewen MacAskill, *NSA PRISM Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[53] Greenwald, *supra* note 52.; *Verizon Forced to Hand Over Data – Full Court Ruling*, GUARDIAN (June 5, 2013, 11:40 PM), https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[54] GUARDIAN, *supra* note 53.
[55] Gellman & Poitras, *supra* note 52.

PRISM, collected audio, video, photos, e-mails, documents, and connection logs, which were analyzed by agency analysts in efforts to track foreign targets.[56] The released top-secret documents showed that the FBI had maintained servers connected to those of private companies including Google, Facebook, Apple, Microsoft, and YouTube, and that this was the number one source of raw signals intelligence used by the NSA for analytic reports.[57] While the intelligence community was not supposed to focus surveillance activities on Americans, target communications likely flowed into and through the United States due to the layout of the global telecommunications backbone.[58] These disclosures highlighted how surveillance, once focused on individual targets, had evolved to surveillance techniques of mass data collection which could incidentally collect information of American citizens.[59]

Congress passed the United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("FREEDOM Act") in response to the Snowden disclosures and the subsequent public outcry.[60] The FREEDOM Act prohibits the type of bulk records collection previously performed under PATRIOT Act authority.[61] But, critics have stated that the FREEDOM Act did not address the "underlying structural wrongs" of government surveillance, and that Congress just "replaced one broad and ambiguous statutory directive with another."[62] In a prescient statement, the Church Committee had found that "[t]he standards

[56] *Id.*
[57] *Id.*; *NSA Slides Explain the PRISM Data-collection Program*, WASH. POST (June 6, 2013), https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents; Barton Gellman and Todd Lindeman, *Inner workings of a Top-secret Spy Program*, WASH. POST (June 29, 2013), https://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282.
[58] WASH. POST, *NSA slides*, *supra* note 57.
[59] Gellman & Poitras, *supra* note 52.
[60] Pub. L. No. 114-23, 129 Stat. 268 (2015); H.R. Rept. No. 114-109, pt. 1 at 2-10 (describing the Snowden disclosures as the impetus of the legislation).
[61] H.R. Rept. No. 114-109, pt. 1 at 2.
[62] Mondale et al., *supra* note 1, at 2275.

governing the use of these [surveillance] techniques have been imprecise and susceptible to expansive interpretation."[63] The same problems still exist today.

C. *State Secrets Doctrine Case Law*

Since 9/11, there has been a significant increase in government invocation of state secrets privilege.[64] These claims have been especially noticeable in cases involving the CIA's extraordinary rendition program and NSA surveillance programs.[65] This section will focus on the use of state secrets privilege in the second context – surveillance programs. Courts have failed to employ "meaningful adversarial testing" or sufficient "inquisitorial review," which has largely endorsed government secrecy decisions and prevented plaintiffs from having a means to seek redress from the government.[66]

The following sub-sections highlight three important cases regarding state secrets privilege. The first, *United States v. Reynolds*, established modern state secrets privilege.[67] In the second, *Fazaga v. FBI*, the Supreme Court held that § 1806(f) does not displace state secrets doctrine.[68] The third, *Wikimedia v. NSA*, dealt with when a plaintiff can use § 1806(f)'s ex *in camera* and *ex parte* review procedures.[69] Both *Fazaga* and *Wikimedia* dealt with plaintiff's alleging that their constitutional rights had been violated by surveillance carried out under FISA Section 702.

---

[63] *Church Committee Report* at 185.
[64] Kwoka, *supra* note 5, at 118.
[65] *Id.*; Press Release, Patrick Leahy, U.S. Senate, Examining the State Secrets Privilege: Protecting National Security While Preserving Accountability (Feb. 13, 2008), https://www.leahy.senate.gov/press/examining-the-state-secrets-privilege-protecting-national-security-while-preserving-accountability. For an example of state secrets privilege and the CIA's extraordinary rendition program, *see* El-Masri v. United States, 479 F.3d 296 (2007).
[66] Kwoka, *supra* note 5, at 118 (2017).
[67] *See* United States v. Reynolds, 345 U.S. 1 (1953).
[68] Fed. Bureau of Investigation v. Fazaga, 142 S. Ct. 1051, 1059 (2022).
[69] *See* Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276 (2021).

1. United States v. Reynolds (1953)

The *Reynolds* decision serves as the foundational case for modern states secrets privilege.[70] *Reynolds* dealt with a military aircraft that had crashed while testing "secret electronic equipment."[71] Three civilian observers were on board the aircraft and died in the crash, and their widows brought suit against the United States and requested production of the Air Force's official accident investigation.[72] In response the government claimed that the aircraft was engaged in a highly secret mission and production would threaten national security.[73] The district court ruled in favor of the plaintiffs when the Government refused to hand over the requested report, and following circuit court's affirmation the case was appealed to the Supreme Court.[74]

The Supreme Court in *Reynolds* described states secrets privilege as one which "is not to be lightly invoked," and it is up to the court to determine if the circumstances of the case are such that the claim is appropriate.[75] The Court called this a "formula of compromise."[76] On the one hand, "judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers."[77] On the other hand, courts may not "automatically require a complete disclosure to the judge before the claim of privilege will be accepted[.]"[78] The latter situation would occur where the government can show that there is a reasonable danger that disclosure to a judge would risk national security.[79] Where a judge is satisfied that national security interests are at stake, "even the most compelling necessity cannot overcome the claim of privilege."[80]

---

[70] *Id.* at 282.
[71] *Reynolds*, 345 U.S. at 3.
[72] *Id.*
[73] *Id.* at 4–5.
[74] *Id.*
[75] *Id.* at 7–8.
[76] *Id.* at 9.
[77] *Reynolds*, 345 U.S. at 9–10 (1953).
[78] *Id.* at 10.
[79] *Id.*
[80] *Id.* at 11.

Ultimately, in the *Reynolds* case, the Court ruled that, while the requested report was certainly privileged, the record did not point to anything showing that the electronic equipment in question had a causal connection to the case, so the plaintiffs should be permitted to proceed without the privileged documents.[81] Decades after the *Reynolds* decision was handed down the requested Air Force accident report was declassified, and it was revealed that the military secrets the government had fought to protect were never included in the report.[82]

2. Federal Bureau of Investigation v. Fazaga (2022)

In *Federal Bureau of Investigation v. Fazaga*, the Supreme Court considered whether § 1806(f) displaces the state secrets privilege and authorizes courts to resolve the merits of a suit after reviewing documents *in camera* and *ex parte*.[83] The plaintiffs, three Muslim residents in California, brought suit against the FBI, claiming that they were illegally surveilled due to their religion.[84] There, the government argued that § 1806(f) is only applicable when a litigant is challenging the admissibility of surveillance evidence put forth by the government.[85] The plaintiffs/respondents argued that § 1806(f) was not restricted to that use case.[86] They argued that § 1806(f) also applies when "an 'aggrieved person' makes 'any motion or request' to 'discover or obtain' electronic-surveillance evidence."[87]

A unanimous Supreme Court declined to resolve the parties' dispute and rule on which meaning of § 1806(f) applies, and instead decided that state secrets privilege is not displaced by § 1806(f).[88] The Court based its decision first on statutory interpretation, stating that the lack of

[81] *Id.*
[82] Report of Special Investigation of Aircraft Accident Involving TB-29-100XX No. 45-21866, available at https://sgp.fas.org/othergov/reynoldspetapp.pdf (last visited May 11, 2023).
[83] 142 S. Ct. 1051, 1056 (2022).
[84] *Id.*
[85] *Id.* at 1059.
[86] *Id.*
[87] *Id.* at 1059 (internal citations reference statutory language of § 1806(f)).
[88] *Id.*

reference to state secrets privilege in FISA and the text of § 1806(f) is evidence against displacement.[89] The Court then reasoned that nothing in § 1806(f)'s operation, even if taking the plaintiff/respondents position, is incompatible with state secrets privilege.[90] This is because, according to the Court, the inquiries undertaken under § 1806(f) and an invocation of state secrets privilege are "fundamentally different."[91] Whereas the § 1806(f) focuses on the lawfulness of government surveillance, a state secrets privilege inquiry focuses on whether disclosure of evidence would risk national security, without regard for the lawfulness of it.[92] The takeaway from the *Fazaga* holding is that § 1806(f) does not require *in camera* review of requested sensitive information in civil litigation challenging the lawfulness of government surveillance.

3. Wikimedia v. National Security Agency/Central Security Service (2021) and subsequent petition to the Supreme Court

Wikimedia v. NSA, which was decided by the Fourth Circuit prior to the Supreme Court's ruling in *Fazaga*, also considered § 1806(f) and its relation to state secrets privilege.[93] Wikimedia filed a civil suit against the NSA, claiming that the agency had spied on their communications using Upstream, an NSA electronic surveillance program.[94] Here, the Fourth Circuit held that while Wikimedia successfully established a genuine issue of material fact sufficient to establish standing, continued litigation would risk national security and state secrets privilege required the suit to be dismissed.[95]

The NSA's Upstream electronic surveillance program at issue in *Wikimedia* operates differently from the PRISM. Whereas PRISM collects data through the assistance of Internet

[89] *Fazaga*, 142 S. Ct. at 1060.
[90] *Id.* at 1061.
[91] *Id.*
[92] *Id.*
[93] *See generally Id.* 1051; Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276 (2021).
[94] *Wikimedia*, 14 F.4th at 279.
[95] *Id.* at 279–78.

Service Providers, such as Google or Facebook, Upstream works by acquiring data from telecommunications backbone providers.[96] These are a high-speed, high-bandwidth lines that travel in and out of the United States and operate as the underlying infrastructure of the global internet, also referred to as "chokepoint" cables.[97] The NSA used these cables to monitor targets and their "selectors," or the means a target uses to communicate and "tasks" them for collection by the telecommunications provider.[98] If a communication is to, from, or (until 2017) about a tasked selector and, critically, at least one end of the communication is foreign, the NSA will gather the communication.[99]

Wikimedia and other plaintiffs sued the NSA on the grounds that the Upstream program violates both First and Fourth Amendment protections, seeking a declaration of such and a permanent enjoinment from conducting the surveillance, as well as an order for the NSA to purge any records of Wikimedia's communications gathered by the program.[100] The court stated that Wikimedia had originally shown standing because:

> (1) its communications travel across every international Internet link; (2) the NSA conducts upstream surveillance on at least one such link; and (3) in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link.[101]

While the Fourth Circuit agreed with Wikimedia that they had established standing, they did not agree with their assertion that § 1806(f) displaces state secrets privilege.[102] The court instead sided with the government's claim that § 1806(f) applies "only when a litigant challenges the admissibility of the government's surveillance evidence," even assuming that Wikimedia is an

[96] Privacy and Civil Liberties Oversight Board, *supra* note 50, at 35; Gellman & Poitras, *supra* note 52.
[97] Privacy and Civil Liberties Oversight Board, *supra* note 50, at 35; *Wikimedia*, 14 F.4th at 280.
[98] *Wikimedia*, 14 F.4th at 280.
[99] *Id.* (citing Privacy and Civil Liberties Oversight Board, *supra* note 50, at 39).
[100] *Id.* at 281.
[101] *Id.* (internal citation and quotations omitted).
[102] *Id.* at 294.

"aggrieved person" as defined in FISA.[103] The § 1806(f) *in camera* and *ex parte* procedures are triggered "only when an aggrieved person is making a motion *in response* to the government's attempt to use . . . FISA documentation and the resulting intelligence" in a proceeding.[104] The Fourth Circuit, while acknowledging that there was a possibility that plaintiff's will be denied legal remedies in the interest of national security, dismissed Wikimedia's argument that limiting the use of § 1806(f) would lead to surveillance abuse by essentially giving the government the ability to dismiss any FISA suit.[105] Here, the court stated that "there is simply no conceivable defense to the assertion [that the NSA is surveilling and acquiring all communications on a monitored chokepoint cable used by Wikimedia] that wouldn't also reveal the very information that the government is trying to protect: how Upstream surveillance works and where it's conducted," and because the "methods and operations" of the NSA are a state secret, the case must be dismissed.[106]

In August of 2022, Wikimedia filed a petition for writ of certiorari to the Supreme Court.[107] Wikimedia argued that, per *Reynolds* and its progeny, state secrets privilege is an evidentiary privilege that, when invoked successfully, excludes the privileged evidence from the litigation but allows the parties to continue litigating with unprivileged evidence.[108] But, even if a court can dismiss a case where a plaintiff can make a prima facie case with nonprivileged evidence, the court must first review the evidence *in camera* to determine if confidential information would truly provide the government with a legally meritorious defense.[109]

Wikimedia contended that the lower courts had essentially, and mistakenly, turned the *Reynolds* holding and state secrets privilege into an immunity doctrine, placing government

[103] *Id.* at 294–96.
[104] *Wikimedia*, 14 F.4th at 297 (emphasis in original).
[105] *Id.* at 300–01.
[106] *Id.* at 304.
[107] Petition for a Writ of Certiorari, Wikimedia Found. v. NSA/Central Sec. Serv., (No. 22-190).
[108] *Id.* at 4.
[109] *Id.* at 4–5.

policies, particularly the intelligence agencies' surveillance practices, beyond the reach of constitutional institutions, even when a plaintiff can establish government liability without the privileged information.[110] They argued that the lower courts have ignored the warnings of *Reynolds* and handed "judicial control over the evidence . . . to the caprice of executive officers."[111] Further, they argued the position that federal courts are well positioned and well versed in handling issues of national security and confidential information.[112] The lower courts have embraced this concerning trend of dismissals despite the fact that in the daces since *Reynolds* trial courts have become well versed in assessing claims involving classified material and national security concerns.[113] Examples of judicial review of sensitive materials include the Freedom of Information Act,[114] FISA electronic surveillance approval procedures,[115] and the Classified Information Procedures Act.[116] In formulating these procedural protections of classified and secret information, "Congress has clearly recognized that courts . . . have demonstrated that they can securely handle secret information in the context of litigation."[117]

The government's response was emblematic of its attempt to use the state secrets privilege to avoid judicial scrutiny and skirt attempts to remedy constitutional violations. In regard to Wikimedia's interpretation of the state secrets doctrine, the government responded that a state secrets dismissal is a "reflecti[on] that the relevant claim is beyond judicial scrutiny because its full adjudication would inevitably lead to the disclosure of matters which the law itself regards as

[110] *Id.* at 15.
[111] *Id.* at 16 (citing United States v. Reynolds, 345 U.S. 1, 9–10 (1953)).
[112] Petition for a Writ of Certiorari, Wikimedia Found. v. NSA/Central Sec. Serv., 19–20 (No. 22-190).
[113] *Id.* at 19.
[114] 5 U.S.C. §§ 552(a)(4)(B), (b)(1).
[115] 50 U.S.C. § 1805.
[116] 18 U.S.C. App. 3.
[117] Petition for a Writ of Certiorari, Wikimedia Found. v. NSA/Central Sec. Serv., 20 (No. 22-190).

confidential."[118] Further, *in camera* review would "jeopardize the security of information."[119] Essentially, the government argued that disclosure of classified material to a judge would negate the very type of action that state secrets doctrine is supposed to protect.[120]

Notably in the *Wikimedia* litigation, the government raised the argument that it may use state secrets privilege to dismiss a case even when a plaintiff can make its case without the confidential, privileged information it seeks.[121] Here, the government relied on a narrow justiciability bar originally applied to claims that relate to secret government contracts in *Totten v. United States* and later *Tenet v. Doe*.[122] In *Totten*, the Court held that "public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential."[123] But the Court in *Tenet* confirmed that *Totten* "precludes judicial review in cases . . . where success depends upon the existence of their secret espionage relationship with the Government."[124] The average American citizen or organization has not entered into an "espionage relationship" with the government, and therefore this doctrine should not be applied to cases where a plaintiff is seeking redress or challenging the legality of surveillance. The attempted expansion of the *Totten and Tenet* doctrines has been a legal argument advanced by the government since the Bush administration in early post-9/11 surveillance and extraordinary rendition cases.[125] This is seen by some as "an attempt to deprive courts of subject matter jurisdiction over cases challenging the constitutionality of certain executive practices" which will "prevent injured parties from vindicating their

[118] Brief of respondents National Security Agency, et. al. in opposition, Wikimedia Found. v. NSA/Central Sec. Serv., 28 (No. 22-190).
[119] *Id.*
[120] *Id.* at 29.
[121] Reply Brief for petitioner Wikimedia Found., Wikimedia Found. v. NSA/Central Sec. Serv., 8 (No. 22-190).
[122] *Id.* at 8–9; *see* 92 U.S. 105 (1875); 544 U.S. 1 (2005).
[123] Totten v. United States, 92 U.S. 105, 107 (1875).
[124] Tenet v. Doe, 544 U.S. 1, 8 (2005).
[125] Frost, *supra* note 5, at 1950–51.

constitutional rights, and will strip the courts of their authority to remedy such violations in individual cases."[126]

The Supreme Court denied Wikimedia's petition for certiorari in February of 2023, leaving open the question of just how far the scope of the state secrets privilege extends.[127] But, the Court's refusal to review the Fourth Circuit's decision could be interpreted as tacit approval of a state secrets privilege that is broad in its application. This perhaps ignores the *Reynolds* Court's direction that state secrets privilege is one which "is not to be lightly invoked."[128]

III. CONGRESS SHOULD AMEND 50 U.S.C. § 1806(F) TO REQUIRE *IN CAMERA* REVIEW WHEN A PLAINTIFF CHALLENGES BRINGS A CIVIL SUIT AGAINST THE GOVERNMENT FOR ILLEGAL SURVEILLANCE

Without judicial review of the government's claim of state secrets privilege, "[h]ow does the [c]ourt know that [they] have a reasonable basis in necessity?"[129] When a plaintiff challenges the lawfulness of government surveillance, and the government invokes state secrets privilege, the trial court judge must be able to review the information in question to determine whether disclosure of the information truly presents a national security risk. Congress should amend § 1806(f) to explicitly require *in camera* review of sensitive information when the government invokes state secrets privilege in civil suits alleging unlawful surveillance. As a result of the federal courts current interpretation of state secrets doctrine, the United States government essentially has a trump card that enables them to have almost any suit against them alleging unconstitutional or

[126] *Id.* at 1951.
[127] *See* Wikimedia Found. v. Nat'l Sec. Agency/Central Sec. Serv., 143 S. Ct. 774 (2023) (denying Wikimedia's petition for writ of certiorari).
[128] *See* United States v. Reynolds, 345 U.S. 1, 7 (1953).
[129] Korematsu v. United States, 323 U.S. 214, 245 (Jackson, J., dissenting).

otherwise illegal surveillance dismissed. That position is antithetical to the concept of checks and balances that is inherent in the American Constitution.

Judicial acquiescence leads to inaccurate outcomes and undermines the law.[130] Continued approval of state secrets privilege undermines the law in two ways: first, failure to submit national security claims to adversarial testing may lead the judiciary to lose legitimacy; and second, continual approval of the doctrine endorses "secret law," which is antithetical to the idea of an open, transparent democracy.[131] Secrecy is indeed vital to national security, especially in the context of surveillance where its success is dependent on secrecy both in its action and its procedures, which may result in less pressure on the government to justify their actions compared to more overt activities like detention and targeting.[132] In fact, the Church Committee acknowledged that "details about military activities, technology, sources of information and particular intelligence methods are secrets that should be carefully protected."[133] But secrecy can limit the ability of Americans to critique the effectiveness of government, and when the judiciary lends extreme deference to the government's state secrets privilege claims it exacerbates this problem, disrupting the system of checks and balances necessary to ensure the intelligence communities do not abuse their power, in contradiction to the warnings of the Church Committee.[134] This Section will discuss how and why Congress should remedy the situation so that those who have been wrongly surveilled may obtain justice.

---

[130] *Id.* at 149.
[131] *Id.* at 149.
[132] Jonathan Hafetz, *A Problem of Standards: Another Perspective on Secret Law*, 57 WM. & MARY L. REV., 2141, 2176 (2016).
[133] SEN. REP. NO. 94-755, Book I, at 13 (1976).
[134] *See* Leahy, *supra* note 65. *See generally*, *Church Committee Report*.

A. Secrecy and Distrust

Secrecy around government actions leads to public distrust. Further, national security is a topic that impacts all Americans, and the citizenry wants to know that its government is properly and efficiently using its resources to ensure the safety of Americans. When it comes to intelligence, naturally the activities of the intelligence agencies are shrouded in secrecy. And, as a former CIA intelligence officer once said, "the secret of our success is the secret of our success."[135] That is, the reason that intelligence agencies can be successful is because their sources and methods are kept secret. The National Security Act of 1947 gave the Director of National Intelligence the responsibility to protect intelligence sources and methods.[136] In proposing a change to FISA § 1806(f), it would be remiss to ignore the successes of Section 702 surveillance. After all, when intelligence surveillance reform efforts began, the Church Committee stressed that civil liberty protections must be balanced with legitimate national security concerns.

At a recent defense panel, Senator Angus King, member of the Senate Select Committee on Intelligence, asked how the intelligence community demonstrates to the public that "the dog . . . didn't bark in the night?"[137] The question is a common one—how do we know Section 702 surveillance is working? Director of National Security General Paul M. Nakasone took up the Senator's question the following month in early 2023 at the Privacy and Civil Liberties Oversight Board Public Forum on FISA Section 702, providing specific examples of how "intelligence acquired under [Section 702] authority has stopped significant terrorist plots, saving American lives."[138] In 2009, Section 702 acquired information was passed to the FBI and led to the arrest of

---

[135] Susan Seligson, *CIA Veteran Hulnick Slam's Agency's Critics*, BU TODAY (Jan. 22, 2010), https://www.bu.edu/articles/2010/cia-veteran-hulnick-slams-agencys-critics.
[136] Pub. L. No. 80–253.
[137] Reagan Foundation, *Reagan National Defense Forum 2022: Panel 2 – Redefining Warfare*, YOUTUBE, (Dec. 4. 2022), https://www.youtube.com/watch?v=LblB917dlzE.
[138] Keynote Speech by Gen Paul M. Nakasone at the Privacy and Civil Liberties Oversight Board Public Forum on FISA Section 702, National Security Agency/Central Security Service, (Jan. 12, 2023), https://www.nsa.gov/Press-

Najibullah Zazi and his co-conspirators, who had planned to detonate explosives on New York City subway trains.[139] In 2014, Section 702 provided intelligence which led to the removal of ISIS leader Hajji Iman and prevented attacks.[140] It also led to the much publicized successful operation to remove one of the last remaining architects of the 9/11 attacks, Ayman al-Zawahiri.[141]

It should be no surprise that the government would highlight its successes in the face of criticism, and examples like the above show that Section 702 may bring about the intended results in at least some cases. But that should not be a basis for excluding reform efforts aimed at ensuring that adequate recourse is available when abuses, intentional or not, do occur. When Congress evaluates FISA for renewal later this year, in addition to the program's success, they need to contemplate what statutory reforms are required for when citizens are negatively impacted by surveillance.

B. Congress Should Review Key Procedures from the Classified Information Procedures Act and Consider Extending Them to Civil Litigation Procedures Under FISA.

Article III judges have experience handling and managing classified information in cases that can be drawn upon when evaluating amendments to § 1806(f). In particular, the Classified Information Procedures Act (CIPA), which was created "[t]o provide certain pretrial, trial, and appellate procedures for criminal cases involving classified information."[142] In addition to dealing with "graymail," a situation where a criminal defendant may seek to introduce classified information related to their case in their defense in order to influence the government to drop their case, CIPA was also envisioned to cover situations where classified information may be material

Room/News-Highlights/Article/Article/3266166/keynote-speech-by-gen-paul-m-nakasone-at-the-privacy-and-civil-liberties-oversi.

[139] NSA, *supra* note 138.

[140] *Id.*

[141] *Id.*

[142] Pub. L. 96-456.

to a defendant's case or where exclusion of such information would violate a defendant's constitutional rights.[143]

While originally intended for criminal cases, these procedures can serve as a model for the civil litigation realm where a plaintiff brings suit and it faced with government invocation of state secrets privilege. CIPA contains procedures that are "intended to create opportunities to resolve issues related to the use of classified information . . . in a secure setting.[144] For example, protective orders may be issued by courts to prevent disclosure of classified information.[145] The protective orders sometimes limit access to individuals and attorneys who have received security clearance, limit access to a defendant's attorney if the defendant is unable to obtain the requisite clearance, or appoint counsel if the defendant's attorney is unable to obtain clearance.[146] CIPA also allows the prosecution to request approval to provide a redacted or substitute version of requested classified information during discovery.[147] The judge will then review the redacted or substitute information and make an *in camer*a and *ex parte* determination of whether or not it is a sufficient proxy for the original.[148] The statutory standard for whether substitution is sufficient is whether it will provide the defendant "with substantially the same ability to make his defense as would disclosure of the specific classified information."[149]

CIPA procedures have been in place since 1980.[150] Thus, the federal judiciary has decades of experience with the procedures, and rules are in place to deal with national security-related classified information in the trial courts. These statutory *in camera* and ex *parte* procedures for

[143] Todd Garvey and Edward C. Liu, CONGRESSIONAL RESEARCH SERVICE, PROTECTING CLASSIFIED INFORMATION AND THE RIGHTS OF CRIMINAL DEFENDANTS: THE CLASSIFIED INFORMATION PROCEDURES ACT, 1 (2012).
[144] Garvey & Liu, *supra* note 143, at 2.
[145] *Id*. at 3.
[146] *Id.*
[147] 18 U.S.C. app 3, §4.
[148] Garvey & Liu, *supra* note 143, at 5.
[149] 18 U.S.C. app 3, §6(c)(1).
[150] Pub. L. 96-456.

review of classified material should serve as a model for Section 702 for civil cases. In the above referenced *Wikimedia* litigation, a group of former Article III judges filed an amicus brief in support of Wikimedia's petition for writ of certiorari to the Supreme Court, arguing that "judges are well-equipped to evaluate assertions of privilege in a national security context with an appropriate level of deference, and that limiting review of privilege claims can lead to costly mistakes."[151] This brief demonstrates that the federal judiciary is capable of handling procedures that would accompany an amendment to § 1806(f) requiring *in camera* review of sensitive material when Section 702 surveillance is challenged.

C. United States v. Zubaydah *and Justice Gorsuch's Dissenting Take on the State Secrets Privilege: a Warning, and What Congress Can Learn from it*.

In *United States v. Zubaydah*, Justice Gorsuch warned in his dissent that recent history should provide a cautionary tale, given the increased in invocation of the state secrets privilege post-9/11. In the aftermath of the September 11th attacks, Zubaydah was believed to be a senior leader of al-Qaeda with knowledge of future attacks against the United States.[152] He was taken into custody, and after transfer between multiple CIA detention sites he was eventually transferred to Guantanamo Bay in September 2006 where he has remained since.[153] Zubaydah claimed that one of these detention sites was located in Poland.[154] Zubaydah initiated a suit Poland, the alleged location of a CIA detention site, seeking to hold officials involved in his alleged mistreatment responsible. Polish prosecutors requested information from the United States under a Mutual Legal Assistance Treaty, which the United States refused under the claim that proving the information

[151] Brief of Former Federal Judges as Amici Curiae in Support of Petitioner, Wikimedia Found. v. NSA/Central Sec. Serv., 1 (No. 22-190).
[152] United States v. Zubaydah, 142 S. Ct. 959, 964 (2022).
[153] *Id.*
[154] *Id.* at 965.

sough would present national security risks.[155] Zubaydah's lawyers then filed an *ex parte* discovery application under 28 U.S.C. § 1782, which provides that a district court may order one the provision of documents for use in foreign tribunals.[156] The government intervened, claiming states secrets privilege.[157] Among the information sought by Zubaydah was confirmation that one of the detainment centers where he was held was in fact located in Poland, which had been made public through unofficial sources,.[158] Details regarding the detention site's location in Poland has been made public through unofficial sources, but the district court nonetheless dismissed the case because it would not be possible to conduct "meaningful discovery . . . without disclosing . . . protected types of information."[159] A divided Ninth Circuit agreed that state secrets privilege did not apply to publicly known information, but disagreed that the case should be dismissed and reversed in part.[160] The Supreme Court disagreed with the lower courts and, applying the Reynold standard, held that "confirmation of that information could reasonably be expected to significantly harm national security interests."[161]

In *Zubaydah*, the Court gave the utmost deference to the government's judgment as to what may be considered a national security risk, and seemingly approved the use of state secrets privilege to avoid admitting to information that was well established in the public realm. Justice Gorsuch, in his dissenting opinion, stated, "[e]nding this suit may shield the government from some further modest measure of embarrassment. But respectfully, we should not pretend it will safeguard any secret."[162] The information sought by Zubaydah has been presented in numerous

[155] *Id.* at 965.
[156] *Id.*; 28 U.S.C. § 1782(a).
[157] *Zubaydah*, 142 S. Ct. at 966.
[158] *Id.*
[159] *Id.* (internal quotations omitted).
[160] *Id.*
[161] *Id.* at 970.
[162] *Id.* at 985 (Gorsuch, J., dissenting).

forums in the years leading up to the case, including a Senate Select Committee report with details of his detention, a European Court of Human finding that it was "'beyond reasonable doubt' that Zubaydah was detained in Poland," and an admission from the former President of Poland that the CIA site was "established 'with [his] knowledge.'"[163] Indeed, "officials can sometimes be tempted to misuse claims of national security to shroud major abuses and even ordinary negligence from public view," such as the infamous *Korematsu* case, where "the President persuaded [the] Court to permit the forced internment of Japanese American citizens during World War II."[164] There, the military report relied to justify the detention measures contained information that executive officials knew to be false, yet the government would not acknowledge its misrepresentation for decades.[165] Even in *Reynolds*, from which we get our modern day privilege doctrine, the Court accepted the government's claim of national security risk "without even pausing to review the report independently in chambers or asking a lower court to take up that task," and then "[d]ecades later, when the government released the report, it turned out to contain no state secrets–only convincing proof of governmental negligence."[166] This begs the question, could such abuses be with *in camera* judicial review? Justice Gorsuch seemed to think so, and presents a compelling framing of the *Reynolds* standard and how judges should evaluate instances of the state secrets privilege going forward in order to prevent such abuses.

First, should the Executive seek to invoke state secrets privilege from a "congressionally authorized judicial proceeding, it must show a 'reasonable danger' of harm to national security would follow" if the privilege were denied.[167] Justice Gorsuch believes that there should be a

[163] *Id.* at 987. For a details on the European Court of Human Rights findings and the conditions Abu Zubaydah was subjected to, *see* 7511/12 Eur. Ct. H.R. (2014).
[164] *Zubaydah*, 142 S. Ct. at 992–93 (Gorsuch, J., dissenting); *see also* Korematsu v. United States, 323 U.S. 214 (1944).
[165] *Zubaydah*, 142 S. Ct. at 993 (Gorsuch, J., dissenting).
[166] *Id.*
[167] *Id.* at 994.

"degree of independent judicial review" of the claim, while also maintaining respect for the "executive's specially assigned constitutional responsibilities field of foreign affairs."[168] Note that Gorsuch does not specifically address instances where a United States citizens' rights are impacted, but "foreign affairs" are likely to be a predicate for any invocation of the state secrets privilege in an illegal surveillance claim as that surveillance would presumably have been, at least officially, aimed at foreign targets. Second, "when assessing a state secrets claim courts may–and often should–review the evidence supporting the government's claim of privilege *in camera*."[169] While the *Reynolds* Court did not consider *in camera* review a requirement, it did stress that a judge must "be satisfied that a reasonable danger of harm would flow from its production."[170] Justice Gorsuch does not go so far as to require *in camera* review, stating that "[a] court [may be] persuaded that the government has met its burden by declaration," but "a court harboring questions must probe further and examine the bases for the government's assertions *in camera*" and may not "allow the government to deny access to every man's evidence unless and until it establishes its lawful entitlement to do so."[171] Justice Gorsuch goes on to highlight statutory procedures put in place by Congress to deal with national security concerns in litigation, including CIPA and FISA §1806(f), and how courts "routinely" test privilege claims.[172] Third, the state secrets privilege "does not prevent a litigant from insisting that the government produce nonprivileged evidence . . . [*n*]*or does the privilege preclude a litigant from pursuing its case otherwise* . . . [as the Executive's national security interest] does not extend to quashing suits that Congress has

[168] *Id.*
[169] *Id.*
[170] *Id.* at 995.
[171] *Zubaydah*, 142 S. Ct. at 995 (Gorsuch, J., dissenting).
[172] *Id.* Note that one day after his dissent in *Zubaydah*, J. Gorsuch would join the majority opinion in *Fazaga* in holding that FISA §806(f) does not override the state secrets privilege, see Fed. Bureau of Investigation v. Fazaga, 142 S. Ct. 1051 (2022).

authorized the Judiciary to entertain."[173] Fourth, should the government properly invoke the privilege, courts "may still be able to make the government's evidence available to litigants in some form as long as it fully respects the government's national security interests."[174] Justice Gorsuch again points to procedures followed under CIPA and FISA §1806(f), as well as lower courts appointing special master to provide summaries to litigants who lack security clearance.

Interestingly, Justice Gorsuch did not dissent from the denial of cert in *Wikimedia*. Perhaps his view on the limits of state secrets privilege in *Zubaydah* is more narrow, as that case dealt with information that had largely been made public by independent sources. The same cannot be said of every intelligence surveillance program. The notion of using the state secrets privilege to cover up information that may be seen as embarrassing, or at least something that the government would prefer to avoid talking about in any official capacity at all, presents a compelling point – that the state secrets privilege was meant to protect government *secrets*, not protect the government from embarrassment or avoid owning its mistakes. In the two decades since 9/11 there have been numerous disclosures, including those made by Edward Snowden, to the point where it has practically become common knowledge that the United States intelligence apparatus casts a very wide net in its surveillance efforts. And it is now an open "secret" that the communications of the average, law-abiding citizen may very well get caught in that net. If in fact there have been Constitutional violations as a result of that net, shouldn't American's be able to seek redress without the government preventing such in order to save face?

[173] *Zubaydah*, 142 S. Ct. at 995–96 (2022) (Gorsuch, J., dissenting) (emphasis added).
[174] *Id.* at 996.

D. Impact of an in camera review requirement on the judiciary

Between 1953 and 1976, there were eleven reported cases of the privilege being raised, and between 1977 and 2001 fifty-nine cases.[175] However, between 2001 and 2006 it was raised twenty times,[176] and between 2006 and 2021 an additional twenty-nine times.[177] In the forty-eight years after *Reynolds*, the privilege was raised seventy times at an average of 1.46 times per year, but in the twenty years since 9/11, it was raised at least forty-nine times at an average of 2.45 times per year.[178] These numbers, even if *in camera* review was required for all instances where state secrets privilege is invoked in a Section 702 cases, do not seem to be at such a volume that would inundate the federal judiciary, especially if the requirement was limited to cases brought against Section 702 surveillance. While there has certainly been an increase in recent years, not all of these cases arose out of claims of illegal surveillance under Section 702. Therefore, requiring *in camera* review of government state secrets privilege claims for cases arising out of FISA Section 702 surveillance is unlikely to inundate the federal judiciary with an additional burden because there will likely be only a few such cases each year.

E. The constitutional authority of the Judiciary to remedy wrongful acts of the Executive

The *Fazaga* holding does not prevent Congress from moving forward with an amendment of § 1806(f). The *Fazaga* holding was based on an interpretation of Congressional intent, and there is nothing stopping Congress from amending the language of § 1806(f) to be more explicit about the procedures the courts must follow, particularly requiring *in camera* review of confidential material, when the government raises the state secrets doctrine.

---

[175] Frost, *supra* note 5, at 1938.
[176] *Id.* at 1939.
[177] Brief for Public Citizen as Amicus Curiae Supporting Respondents, at 9–10, United States v. Zubaydah, 142 S. Ct. 959 (2022) (No. 20-827).
[178] *Id.* at n. 4. The tally for 2006–2021 claims of the privilege includes Freedom of Information Act and CIPA cases.

If the statute is amended as proposed, the government may still invoke state secrets privilege when faced with claims of illegal surveillance by an aggrieved person. But, under the proposed change, federal trial courts would be required to review the information over which the government is claiming privilege *in camera* before ruling that the state secrets privilege is appropriate in the situation, and if so whether the litigation may proceed without the information in question. Perhaps fortuitously, the Supreme Court's denial of cert in the *Wikimedia* means that the Court will not, at least not anytime soon, find the source of state secrets privilege within the Constitution or that it is otherwise far reaching in a way that would prevent statutory empowerment of litigants. Supreme Court caselaw on state secrets privilege has held that, in addition to finding its roots in the common law of evidence, the state secrets privilege does have a basis in the Constitution insofar as it pertains to, or acts as a tool of, the Executive's Constitutional authority over national security concerns. Without the Supreme Court explicitly holding that the state secrets privilege is rooted in the Constitution, it is unlikely to hold that it can serve as a blanket privilege—in other words, a trump card—that can be used to dismiss any case brought before it that implicates national security concerns. The Court's opinions since *Reynolds* have held that state secrets privilege must be raised properly and when there is a reasonable danger of harm to national security. There have been differing opinions, highlighted in *Zubaydah*, as to what is considered reasonable a reasonable danger. With the denial of cert in *Wikimedia*, a role for Congress is unlikely to be ruled out any time soon. The proposed amendments to §1806(f) would serve to ensure that the courts have a role in determining that the privilege is not "invoked lightly" by performing *in camera* review of the information in question.

Of concern, however, is if an opportunity were to arise for the Court to extend the *Tenet/Totten* doctrine and create a justiciability bar for cases dealing with government surveillance

activities. Should the Court extend the *Tenet/Totten* doctrine, it would take away lower courts' jurisdiction to take up cases challenging government surveillance. Professor Amanda Frost argues that this would be "an unwarranted usurpation of judicial power," and attack on not only "the rights of individuals, but on the jurisdiction-conferring authority of the legislature."[179] Professor Frost has, in her article on state secrets privilege and the separation of powers, invoked the functionalist approach typified in Justice Jackson's concurrence in *Steel Seizure* case – that "there are no bright lines demarcating the roles of the three branches; their powers are shared, so oftentimes one branch must obtain another's approval before acting."[180] Frost proposes that when an executive program is challenged for abuse of power, "courts should hesitate to abandon the field unless Congress is willing to step in."[181] I propose that Congress should act by explicitly designating that power to the judiciary to review of the executive's claims when they invoke state secrets privilege against claims of illegal surveillance through *in camera* review of the confidential information requested by a plaintiff. Ever since the Church Committee's findings and recommendations, the passing of FISA, and FISA's subsequent amendments, the executive branch has evolved its surveillance capabilities and programs to sidestep the procedural and legal barriers that Congress has put in place. With each Congressional hearing and committee, the Executive finds a new way to carry out its intelligence gathering activities in line with the most recent standards. History shows us that, when it comes to government surveillance, perhaps Congressional oversight of the Executive branch is not enough, and Judicial branch must take on an expanded role to serve as an additional check on Executive power.

[179] Frost, *supra* note 5, at 1932.
[180] *Id.* at 1934; *see also* Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 635–37 (1952) (Jackson, J., concurring).
[181] Frost, *supra* note 5, at 1963.

IV. CONCLUSION

State secrets privilege has served to protect the government from accountability, or, at a minimum, it has protected them from facing aggrieved parties on the merits when accused of constitutional violations or faced with claims of illegal surveillance. At the same time, national security concerns are paramount. Amending FISA § 1806(f) such that the state secrets privilege does not serve as an absolute bar to litigation, but potentially sensitive materials remain under judicial review in a secure setting, will help fulfill the goals initially set out by the Church Committee so many years ago – balancing personal liberty interests with those of national security. This change would accomplish but a small part of the changes needed in the intelligence community's surveillance practices, as the growth of surveillance capabilities, due to technological advances and the ubiquity of the global internet, has likely surpassed what the Church Committee could have imagined in 1975. At that time, the 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."[182]

In conclusion, Congress should explicitly amend § 1806(f) to require *in camera* judicial review of confidential information when the government invokes state secrets privilege. The need for Congressional action is more vital now that the Supreme Court has declined to take up *Wikimedia*, as there will be no judicial roadblocks surrounding the state secrets privilege when FISA comes up for renewal at the end of 2023. Section 702 is likely to be a prime subject of debate, and some members of the 118th Congress have already expressed their concern regarding widespread surveillance. If Congress does not act to reign in the use of state secrets privilege

[182] *Church Committee* at 289.

during FISA renewal talks, it runs the risk of maintaining the status quo or worse leaving the door open to future interpretation of state secrets privilege as an even broader doctrine than it is already widely accepted to be.