Boston College Law Review

Volume 61
Issue 9 *Electronic Supplement*

Article 35

6-9-2020

Want to Know a Secret . . .? Electronic Surveillance, National Security, and the Role of the Foreign Intelligence Surveillance Act

Jesslin Wooliver
Boston College Law School, jesslin.wooliver@bc.edu

WANT TO KNOW A SECRET . . . ? ELECTRONIC SURVEILLANCE, NATIONAL SECURITY, AND THE ROLE OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Abstract: On February 29, 2019, the United States Court of Appeals for the Ninth Circuit held in *Fazaga v. Federal Bureau of Investigation* (*Fazaga II*) that the Foreign Intelligence Surveillance Act (FISA)—passed in 1978 to limit the government's ability to conduct certain surveillance activities without court authorization—displaces the state secrets privilege in all cases involving electronic surveillance for foreign intelligence purposes. Until recently, courts applied the procedures set forth in FISA only to claims brought under FISA. Meanwhile, the state secrets privilege—a common-law doctrine insulating the government from disclosing sensitive information related to national security in court—has long governed the U.S. government's use of electronic surveillance for domestic and foreign intelligence purposes. This Comment examines the conflict between national security and individual liberties underlying FISA and the state secrets privilege. It argues that, in times of unprecedented technological advances, *Fazaga II* appropriately preserves the role of each governing branch in protecting these values.

INTRODUCTION

The Supreme Court first authorized the government to conduct electronic surveillance on its citizens in 1928.[1] Since then, technological advances have only made surveillance easier to exploit and more difficult to detect.[2] Although United States citizens enjoy the constitutional right against unreasonable searches and seizures by the government, the government routinely monitors individuals as they travel, talk on the phone, and browse and communicate online.[3] Though intrusive, electronic surveillance is essential to national secu-

[1] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that the government's unwarranted wiretapping of private citizens does not violate the Fourth Amendment), *overruled by* Berger v. New York, 388 U.S. 41, 50–60 (1967), *and* Katz v. United States, 389 U.S. 347, 353 (1967).

[2] *See* OFFICE OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES, 3, 9 (1985), https://www.hsdl.org/?abstract&did=727025 [https://perma.cc/BQ6Z-BRCU] [hereinafter OFFICE OF TECH. ASSESSMENT] (stating that the "virtual revolution" in electronic surveillance technology that took place between 1965 and 1985 made electronic surveillance easier to conduct and harder to adjudicate).

[3] *See* U.S. CONST. amend. IV. (establishing citizens' right against unreasonable searches and seizures without probable cause); OFFICE OF TECH. ASSESSMENT, *supra* note 2, at 12–14 (providing a historical overview of the government's use of electronic surveillance). For example, police departments and federal agencies across the country operate automatic license plate readers, surveillance cameras, and radiation sensors, and they monitor telephone records and track social media accounts,

rity; intelligence and military operations utilize these technologies to detect and prevent acts of terrorism and other criminal activity.[4] This conflict between national security and personal liberties has long troubled the court system.[5]

The state secrets privilege—a common-law evidentiary privilege allowing the government to withhold otherwise discoverable material when it contains sensitive information regarding national security—is fundamental to the judiciary's treatment of national security cases.[6] Congress also addressed the issue in 1978 when it passed the Foreign Intelligence Surveillance Act (FISA).[7] FISA codified rules and procedures regarding the government's use of electronic surveillance in foreign and domestic intelligence operations.[8]

This Comment explores the state secrets privilege and FISA through the lens of the Ninth Circuit Court of Appeals' 2019 decision in *Fazaga v. Federal Bureau of Investigation* (*Fazaga II*).[9] In *Fazaga II*, the Ninth Circuit held that

---

among much else. Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 13, 2013), https://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html [https://perma.cc/HDK8-6RPD]. This process of gathering as much surveillance information as possible about human activity is known as "data mining." *Id.*

[4] *See* OFFICE OF TECH. ASSESSMENT, *supra* note 2, at 11, 22 (discussing surveillance technology's ability to uncover valuable information in the law enforcement and national security sector and the need to balance individual liberty interests with the government's interest in using electronic surveillance).

[5] *See id.* at 10, 12 (stating that historically Congress, the courts, and the executive branch have balanced society's interest in individual liberties against its interest in national security when considering electronic surveillance policy); *see, e.g.*, *Katz*, 389 U.S. at 354 (rejecting the government's argument that its electronic surveillance of the defendant was justified because the officers had strong reason to believe that the defendant was committing a federal crime); Korematsu v. United States, 323 U.S. 214, 215–16 (1944) (holding that the government was permitted to detain and displace innocent Japanese individuals in order to prevent espionage and sabotage), *abrogated by* Trump v. Hawaii, 138 S. Ct. 2392, 2422 (2018).

[6] *See* Fazaga v. Fed. Bureau Investigation (*Fazaga II*), 916 F.3d 1202, 1226–27 (9th Cir. 2019) (discussing the development of the state secrets privilege); El-Masri v. United States, 479 F.3d 296, 303–04 (4th Cir. 2007) (explaining the constitutional importance of the state secrets privilege allowing the executive branch to protect the secrecy of sensitive government information). As early as 1875, the Supreme Court dismissed a claim against the government due to the potential danger of revealing government secrets if the case were to proceed. *See* Totten v. United States, 92 U.S. 105, 107 (1875) (affirming dismissal of a case where litigation would result in the disclosure of confidential government information).

[7] 50 U.S.C. §§ 1801–1813 (2018).

[8] *Id.* FISA created a procedure for courts to follow when deciding whether some instance of government surveillance activity was lawful. *Id.* § 1806(f). Though this Comment focuses solely on the Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act and the Omnibus Crime Control and Safe Streets Act of 1968 also play a large role in governing electronic surveillance. *See id.* (providing protections for electronic communications and transactions); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (1986) (creating procedures for governmental authorities to gain judicial permission for wiretapping); Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2516 (1968) (permitting government surveillance for criminal law enforcement purposes in certain contexts and in accordance with specific procedures).

[9] 916 F.3d 1202 (2019); *see infra* notes 14–111 and accompanying text.

the judicial review procedure provided in FISA is applicable to all claims arising out of an allegedly unlawful use of electronic surveillance, thus preempting the state secrets privilege for matters relating to electronic surveillance.[10] Part I of this Comment introduces the legal and factual background of *Fazaga II*.[11] Part II discusses how the Ninth Circuit balanced national security concerns with individual liberties and ultimately arrived at its decision.[12] Finally, Part III argues that the Ninth Circuit was correct to overturn the district court's problematic decision and emphasizes the importance of balancing administrative and democratic values in a technologically advanced society.[13]

I. NATIONAL SECURITY, STATE SECRETS, AND FISA

In *Fazaga II*, the Ninth Circuit held that the *in camera* and *ex parte* review procedure set forth in FISA is applicable to all claims arising out of an allegedly unlawful use of electronic surveillance, therefore preempting the state secrets privilege.[14] Section A of this Part explains the legal context underlying the Ninth Circuit's decision, the development of the state secrets privilege, and the enactment of FISA.[15] Section B provides a factual overview of *Fazaga II*.[16] Lastly, Section C recounts the case's procedural history.[17]

A. Legal Context

In March 1953, in *United States v. Reynolds*, the Supreme Court held that the state secrets privilege allows the government to withhold sensitive military or intelligence information from discovery.[18] To succeed on a state secrets

---

[10] 916 F.3d at 1230.

[11] *See infra* notes 14–51 and accompanying text.

[12] *See infra* notes 52–85 and accompanying text.

[13] *See infra* notes 86–111 and accompanying text.

[14] *See* 916 F.3d at 1230–31 (holding that the FISA procedure directly addressed the national security concerns underlying the state secrets privilege and, as a result, that Congress intended for it to displace the privilege). *In camera* refers to a judge's private review of information. *In camera*, BLACK'S LAW DICTIONARY (11th ed. 2019). *Ex parte* refers to a motion that a court considers without hearing from the opposing party. *Motion*, *id.*

[15] *See infra* notes 18–34 and accompanying text.

[16] *See infra* notes 35–41 and accompanying text.

[17] *See infra* notes 42–51and accompanying text.

[18] 345 U.S. 1, 6 (1953). In *Reynolds*, three widows of passengers killed in a military plane crash sued the United States under the Federal Tort Claims Act (FTCA). *Id.* at 3; *see* 28 U.S.C. §§ 1346, 2674 (2018) (providing that the United States government could be found liable "in the same manner" that any private citizen would). When the plaintiffs sought to review the Air Force's official accident record and the surviving crewmembers' statements, the government moved to suppress, claiming that the information was privileged. *Reynolds*, 34 U.S. at 3–4. The District Court for the Eastern District of Pennsylvania and the United States Court of Appeals for the Third Circuit agreed that the plaintiffs had shown good cause for producing the evidence and therefore waived the government's privilege claim, but the Supreme Court reversed. *Id.* at 5–6. The Court concluded that even when there is a demonstrated need for the information, a claim of privilege cannot be overcome if the court deter-

privilege claim, the government must meet three requirements.[19] First, after personally reviewing the material, the head of the relevant government department must formally assert the privilege.[20] The claim must provide enough detail about the basis and scope of the asserted privilege for the court to determine its validity.[21] Second, the court must determine if the information is, in fact, privileged.[22] Though this determination takes the specific circumstances of the case into account, the court must ultimately defer to the government on matters of national security.[23] Third, if the court sustains the claim, it will determine whether the case can proceed without disclosure of the privileged information or if it requires dismissal.[24]

Although the government rarely employed the state secrets privilege in the twenty years following *Reynolds*, the government's use of unauthorized electronic surveillance—and the public's concern over this practice—expanded in the late 1970s.[25] In June 1972, in *United States v. U.S. District*

---

mines that the case poses a risk of disclosing military secrets. *See id.* at 11 (explaining that although courts should consider the importance of the information at issue, they should ultimately defer to the executive branch's assertion of privilege). "Privilege" is defined as "a special legal right, exemption, or immunity granted to a person or class of persons; an exception to a duty." *Privilege*, BLACK'S LAW DICTIONARY, *supra* note 14. [19] *See* Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1202 (9th Cir. 2007) (outlining the three steps to successfully asserting a state secrets privilege claim).

[19] *See* Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1202 (9th Cir. 2007) (outlining the three steps to successfully asserting a state secrets privilege claim).

[20] *Reynolds*, 345 U.S. at 7–8.

[21] *Fazaga II*, 916 F.3d at 1228.

[22] *Reynolds*, 345 U.S. at 8.

[23] *See id.* at 9, 10 (explaining that although a court must first determine that disclosing the information would present a risk to national security if it is to allow the government to assert the privilege, it should not insist on examining the evidence if the government has presented sufficient information to show that disclosure could present a danger to national security); *Al-Haramain*, 507 F.3d at 1203 (stating that the judiciary must "defer to the Executive on matters of foreign policy and national security").

[24] *See Al-Haramain*, 507 F.3d at 1204 (explaining that if information is withheld under the state secrets doctrine, litigation can proceed only if the plaintiffs can prove the facts necessary to their claim without that information); Kasza v. Browner, 133 F.3d 1159, 1170 (9th Cir. 1998) (holding that the privileged information was so essential to the plaintiff's claim that the entire action required dismissal). *Reynolds* distinguished between the evidentiary privilege against disclosing sensitive information—the "*Reynolds* privilege"—and those cases in which the underlying subject matter concerns state secrets and thus requires the complete dismissal of all claims: the "*Totten* bar." *Reynolds*, 345 U.S. at 6–7; *see also Totten*, 92 U.S. at 107.

[25] *See Fazaga II*, 916 F.3d at 1233 (reviewing FISA's legislative history); Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1291–92 (2007) (tracing the evolution of the state secrets privilege). In 1976, a congressional task force revealed that the government had long been conducting unauthorized surveillance and using its findings improperly for years. *See Fazaga II*, 916 F.3d at 1233 (citing SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES & THE RIGHTS OF AMERICANS, S. REP. NO. 94–755, at 290 (1976)). The committee recommended legislation to deter unlawful surveillance and to prevent further abuses of executive authority. *Id*. These findings, however, especially in combination with the Watergate scandal and surrounding media attention, caused public trust in the government to fall dramatically. Chesney, *supra* at 1264.

Court (*Keith*), however, the Supreme Court held that the Fourth Amendment required judicial approval of any electronic surveillance of American citizens, thus limiting the executive's use of the practice.[26] Consequently, litigation over the use of electronic surveillance grew, and the government began asserting the privilege more regularly.[27]

At the suggestion of the Senate Judiciary Committee and Justice Powell in his majority opinion in *Keith*, Congress intervened by enacting FISA in 1978.[28] FISA created rules and procedures for the use of electronic surveillance and established a Foreign Intelligence Surveillance Court to approve government applications for electronic surveillance warrants.[29] Procedurally, FISA gives courts the ability to review *in camera* and *ex parte*—privately and without input from the opposing party—any material necessary to determine whether the government lawfully collected the electronic surveillance information over which it asserts a privilege.[30]

---

[26] 407 U.S. 297, 313–14, 317–18 (1972). The case is commonly referred to as *Keith*, the name of the district judge respondent. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 31:3 (updated Sept. 2019).The Supreme Court had previously established in 1967 in *Katz v. United States* that the Fourth Amendment protection against unreasonable searches and seizures was not limited to physical trespass, but also prevented the government from conducting wiretaps without a warrant. 389 U.S. at 359. In *Keith*, the Court concluded that the government was not excused from this requirement just because the surveillance fell within the broad classification of domestic security. 407 U.S. at 320.

[27] *See* Chesney, *supra* note 25, at 1292 (discussing the increased use of the state secrets privilege). Although courts decided only six cases concerning the state secrets privilege in the nineteen years after Reynolds, they decided sixty-five in the next twenty-nine years. *Id.* at 1297.

[28] *See Keith*, 407 U.S. at 323–24 (noting that judicial approval is necessary for domestic security surveillance and that the sensitive nature of the issue may warrant the creation of a special court by Congress); ELIZABETH B. BAZAN & JENNIFER K. ELSEA, CONG. RESEARCH SERV., R40888, PRESIDENTIAL AUTHORITY TO CONDUCT WARRANTLESS ELECTRONIC SURVEILLANCE TO GATHER FOREIGN INTELLIGENCE INFORMATION 12–13 (2006) (discussing the history of FISA). *See generally* 50 U.S.C. §§ 1801–1813 (creating a new process for courts to follow when dealing with the government's use of electronic surveillance).

[29] *See* 50 U.S.C. § 1806(a)–(g) (limiting the government's ability to disclose information obtained through electronic surveillance); *Fazaga II*, 916 F.3d at 1232 (providing an overview of FISA's structure and specifications). If the government seeks to disclose such information obtained through electronic surveillance, it must follow minimization procedures requiring it to notify plaintiffs of any electronic surveillance information that it intends to enter into evidence. 50 U.S.C. § 1806(a)–(g). FISA also provides that persons against whom the government brings electronic surveillance evidence may move to suppress that evidence if it was not acquired in accordance with FISA. *Id.*

[30] 50 U.S.C. § 1806(f). FISA specifies three situations in which a court is to follow its review procedure: when the government gives notice of its intent to disclose information obtained through electronic surveillance, when a party subjected to unauthorized electronic surveillance moves to suppress information obtained through the surveillance, and when a person subjected to unauthorized electronic surveillance requests to view information relating to its content or usage. *Id.* § 1806(c)–(f). In 1991 in *ACLU Foundation of Southern California v. Barr,* the D.C. Circuit held that when a court reviews material under FISA, it must determine whether the surveillance was lawfully conducted under both FISA and the Constitution. 952 F.2d 457, 465 (D.C. Cir. 1991). In the same year, the First Circuit came to the same conclusion in *United States v. Johnson*. *See* 952 F.2d 565, 571–73 (1st Cir. 1991) (using FISA's review procedure to examine the constitutionality of electronic surveillance).

Plaintiffs trigger FISA review when they invoke the statute to allege an unlawful use of electronic surveillance.[31] When they challenge electronic surveillance on grounds other than FISA, however, the state secrets privilege generally enables the executive branch to withhold information about its activity simply by asserting that the surveillance concerns national intelligence.[32] Indeed, the privilege has been widely criticized for allowing the executive branch to easily avoid judicial review.[33] In *Fazaga II*, the Ninth Circuit addressed these concerns by holding that the judicial review process outlined in FISA applies even in non-FISA claims.[34]

B. Factual Background

In 2006, the FBI hired Craig Monteilh to work as a confidential informant on a counterterrorism probe called Operation Flex.[35] Two FBI agents, Kevin Armstrong and Paul Allen, supervised Monteilh and instructed him to gather information about the Muslim community in Southern California by obtaining Muslim individuals' contact information, befriending them, and placing electronic surveillance equipment in specific locations.[36] Monteilh surveilled the

---

Unauthorized electronic surveillance is lawful under FISA only when it is unlikely to include communications between United States citizens. 50 U.S.C. § 1802(a)(1) (2008).

[31] *See* John J. Dvorske, Annotation, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 190 A.L.R. FED. 385, § 4 (2003) (providing examples of cases involving the scope of FISA and the *ex parte* review of electronic surveillance evidence).

[32] *See Fazaga II*, 916 F.3d at 1226 (stating that no other federal court of appeals had addressed the question of whether FISA displaces the state secrets privilege in non-FISA electronic surveillance claims, such as violations of the Fourth Amendment or the Privacy Act); *see, e.g.*, Abilt v. CIA, 848 F.3d 305, 317–18 (4th Cir. 2017) (dismissing the case under the state secrets privilege); United States v. Schulte, 1:17-CR-00548, 2019 WL 4688707, *4–5 (S.D.N.Y. 2019) (finding that the state secrets privilege protected the relevant information and ordering the government to provide redacted summaries of the documents). The United States District Court for the Central District of California in *Fazaga v. Federal Bureau of Investigation* (*Fazaga I*) held in 2012 that causes of action arising from statutory or constitutional provisions other than FISA are not within FISA's scope and, therefore, are vulnerable to dismissal under the state secrets privilege. *See* 884 F. Supp. 2d 1022, 1037–38 (S.D. Cal. 2012).

[33] *See* Carrie Newton Lyons, *The State Secrets Privilege: Expanding Its Scope Through Government Misuse*, 11 LEWIS & CLARK L. REV. 99, 119 (2007) (arguing that the state secrets privilege is being used to dismiss cases prematurely, thereby interfering with private and public constitutional rights); Paul M. Schwartz, *Warrantless Wiretapping, Fisa Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture*, 97 CAL. L. REV. 407, 429, 432 (2009) (arguing that government transparency and institutional integrity are essential to protecting public liberty); Christina E. Wells, *State Secrets and Executive Accountability*, 26 CONST. COMMENT. 625, 630 (2010) (arguing that the state secrets privilege does not provide the judicial branch with sufficient power to hold the executive branch accountable for misuse of authority).

[34] *Fazaga II*, 916 F.3d at 1230*; see infra* notes 52–85 and accompanying text.

[35] *Fazaga II*, 916 F.3d at 1212.

[36] *Id.* During his time working for Operation Flex, Monteilh helped the FBI obtain "hundreds of phone numbers; thousands of email addresses; background information on hundreds of individuals; hundreds of hours of recordings of the interiors of mosques, homes, businesses, and associations; and

community for over a year, attending daily religious services at the Islamic Center of Irvine (ICOI), as well as prayers, classes, lectures, fundraisers, and other events with members of the Muslim community with whom he had made contact.[37] Monteilh recorded nearly all these interactions, including conversations he had with Sheikh Yassir Fazaga, an imam at a local mosque, and Yasser AbdelRahim, an ICOI congregant.[38]

Once Monteilh assimilated into the Muslim community, Armstrong and Allen instructed him to inquire about jihad and armed conflict and to express interest in taking violent action.[39] In response, ICOI community members reported Monteilh to community leaders who called the FBI and the Irvine Police Department.[40] The ICOI then requested a restraining order against Monteilh and, eventually, his identity as an FBI informant was revealed.[41]

C. Procedural History

In September, 2011, Fazaga, AbdelRahim, and Ali Uddin Malik, another practicing Muslim at the ICOI, filed a class action in the United States District Court for the Central District of California on behalf of all Muslim individuals who Monteilh surveilled during Operation Flex.[42] The complaint accused the government and, separately, the federal agents in their official capacities, of unlawful discrimination and searches, asserting violations of FISA, the First Amendment's Religion Clauses, the Fifth Amendment's Due Process Clause,

---

thousands of hours of audio recordings of conversations, public discussion groups, classes, and lectures." *Id*. He recorded his interactions with a cellphone, two key chains capable of recording audio, and a camera attached to a button on his shirt. *Id.* at 1213. FBI officials later transcribed the recordings. *Id.*

[37] *Id.* at 1212–13. While attending community events, Monteilh collected the names of leaders in the community, license plate numbers from cars in the mosque parking lot, individuals' travel plans and charitable activities, and other information that could be used to recruit additional informants for the FBI. *Id.* at 1213.

[38] *Id.* at 1213, 1218.

[39] *Id.* at 1213–14. Monteilh told several individuals that he could acquire weapons and was willing to engage in violence in the name of his faith. *Id.* at 1214.

[40] *Id*.

[41] *Id.* A court granted the ICOI a restraining order against Monteilh in June of 2007. *Id.* A few months later, the FBI discharged Monteilh from Operation Flex and told him not to speak about the investigation. *Id.* Monteilh's identity as an informant was not revealed until 2009, when one of the ICOI members who he had been in contact with, Ahmadullah Niazi, was prosecuted for naturalization fraud. *Id.* At Niazi's bail hearing, another FBI agent testified that he had heard recordings of Niazi speaking with an FBI informant, the same man who the ICOI had reported to the police. *Id.* Various sources confirmed that Monteilh was the informant in question and that he had been working for the FBI at the time. *Id.* The FBI, though it revealed some information about Monteilh's role in the operation, insisted that the operation was a matter of national security and thus that the details of Monteilh's activities must be kept secret. *Id.*

[42] *Id.* At the time of the Ninth Circuit's decision in *Fazaga II*, the plaintiffs had not yet been certified as a class, partly due to the unresolved nature of the government's assertion of the state secrets doctrine. *Id.*

the Religious Freedom Restoration Act (RFRA), and the Federal Tort Claims Act (FTCA).[43]

In response, both the government and the agents moved to dismiss the claims.[44] The government also moved for summary judgment.[45] It argued that the plaintiffs' claims under the First Amendment, the Due Process Clause of the Fifth Amendment, the Privacy Act, FISA, the Religious Freedom Act, and the Federal Tort Claims Act should be dismissed under the *Reynolds* state secrets privilege because they could not be litigated without risking the disclosure of privileged information.[46]

Although the district court permitted the FISA claim against the agents to proceed, it dismissed all other claims against both the agents and the government.[47] Specifically, the court dismissed the FISA claim against the government, as well as the First Amendment, Fifth Amendment, and RFRA claims against the agents, due to sovereign immunity.[48] The court dismissed the remaining claims, including the Fourth Amendment claim, due to the *Reynolds* state secrets privilege.[49] The court thus rejected the plaintiffs' argument that FISA preempted the invocation of the privilege over these claims, holding that

---

[43] *Id.* The plaintiffs alleged that the government and its agents violated the First and Fifth Amendments of the Constitution by surveilling them because of their religion. *Id.* at 1242. Additionally, the plaintiffs maintained that the defendants violated the Religious Freedom Restoration Act (RFRA) by infringing upon their freedom of religion. *Id.* at 1246. The FTCA claim contended that the government infringed upon the plaintiffs' constitutional rights under California law, including their right to privacy, and also asserted intentional infliction of emotional distress. *Id.* at 1250. The Privacy Act claim alleged that the FBI had unlawfully collected and maintained information regarding the plaintiffs' religious practices. *Id.* at 1248.

[44] *Id.* at 1215.

[45] *Id.*

[46] *Id.*; *see Reynolds,* 345 U.S. at 6–7 (explaining that the privilege against revealing military secrets is well established). The government did not assert the state secrets privilege over the Fourth Amendment claims. *Fazaga II*, 916 F.3d at 1215.

[47] *Fazaga I*, 884 F. Supp. 2d at 1029.

[48] *Fazaga II*, 916 F.3d at 1215. Sovereign immunity is defined as "a government's immunity from being sued in its own courts without its consent." *Sovereign immunity*, BLACK'S LAW DICTIONARY, *supra* note 14. The district court found that Congress had not waived sovereign immunity for damages claims under FISA and therefore dismissed the FISA claim against the government. *Id.* The plaintiffs did not challenge this finding on appeal. *Id.* Regarding the religion claims, the plaintiffs showed that the defendants' conduct caused them to become less inviting to new mosque attendees, to attend mosque less frequently, to donate less to mosque institutions, and, for Fazaga in particular, to abandon his counselling practice for mosque attendees. *Id.* at 1247. Nonetheless, the court held that, at the time of the surveillance, there was insufficient case law to put the defendants on notice that their conduct could contravene the RFRA. *Id.*

[49] *Fazaga II*, 916 F.3d at 1215. The District Court concluded that the disclosure of any information related to Operation Flex, irrespective of whether the information was privileged, would present too great a risk to national security to justify moving forward with the case. *Fazaga I*, 884 F. Supp. 2d at 1029. It reasoned that the government could not defend itself against the plaintiffs' claims without relying on privileged information. *Id.*

FISA procedures apply to FISA claims only.[50] Both the plaintiffs and the agent defendants appealed to the Ninth Circuit.[51]

II. *FAZAGA II*: DISPLACING THE STATE SECRETS DOCTRINE IN ELECTRONIC SURVEILLANCE CASES

In February 2019, in *Fazaga v. Federal Bureau of Investigation* (*Fazaga II*), the Ninth Circuit Court of Appeals overturned the district court's dismissal of the plaintiffs' Fourth Amendment claims.[52] The Ninth Circuit held that the *in camera* and *ex parte* review procedure outlined in the Foreign Intelligence Surveillance Act (FISA) applied to all claims arising out of an allegedly unlawful use of electronic surveillance, precluding the assertion of the state secrets privilege.[53] Section A of this Part explains the court's reasoning in *Fazaga II*.[54] Section B discusses the policy concerns underlying the district court and Ninth Circuit decisions.[55]

A. The Ninth Circuit Clarifies the Proper Role of FISA

Until the Ninth Circuit's decision in *Fazaga II,* no federal court of appeals had addressed whether the procedures outlined in FISA supersede the state secrets privilege.[56] Two district courts, however, previously held that because the state secrets privilege developed as a common-law rule of evidence in the absence of relevant legislation, FISA displaces the privilege on matters addressed in the statute.[57] The Ninth Circuit expanded upon these decisions, explaining that FISA's language and legislative history demonstrate that its

---

[50] *Fazaga I*, 884 F. Supp. 2d at 1038.

[51] *Fazaga II*, 916 F.3d at 1216. The plaintiffs appealed the dismissal of their claims. *Id.* The agents appealed the denial of qualified immunity on the FISA claim. *Id.* The *Fazaga II* court addressed both appeals. *Id.*

[52] 916 F.3d 1202,1225 (9th Cir. 2019) (agreeing with the plaintiffs' contention that the District Court should have utilized the Foreign Intelligence Surveillance Act's procedure in reviewing the purportedly privileged information).

[53] *See id.* at 1238 (concluding that "the plain language, statutory structure, and legislative history" of FISA revealed Congress's intent "to displace the state secrets privilege and its dismissal remedy with respect to electronic surveillance.").

[54] *See infra* notes 56–73 and accompanying text.

[55] *See infra* notes 74–85 and accompanying text.

[56] *See Fazaga II*, 916 F.3d at 1226 (stating that the Ninth Circuit was the first federal court of appeals to address the issue).

[57] *See* Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090, 1105–06 (N.D. Cal. 2013) (finding that FISA was intended to supersede the state secrets privilege in FISA-related issues); *accord In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1120 (N.D. Cal. 2008) (finding that FISA displaces the state secrets privilege when the issue is "within FISA's purview"). It is well established that when Congress enacts legislation that speaks directly to an issue addressed in common law, the common law is displaced. *Fazaga II*, 916 F.3d at 1230 (quoting United States v. Texas, 507 U.S. 529, 534 (1993)).

procedural provisions should not be limited to FISA claims.[58] Rather, they should apply to all claims related to unauthorized electronic surveillance.[59]

First, the Ninth Circuit looked to FISA's language.[60] According to the statute, its procedure for judicial review should apply whenever the government moves to suppress electronic surveillance information requested by the opposing party on the grounds that releasing the information would create a national security risk.[61] This procedure governs regardless of the court in which the motion is brought, and regardless of any other law.[62] Thus, according to the Ninth Circuit, the statute necessarily displaces the usual procedures governing the admission of evidence and the dismissal remedy utilized by the state secrets privilege.[63] Moreover, the FISA review procedure is triggered by circumstances almost indistinguishable from those that precipitate an exercise of the state secrets privilege.[64] For example, if the Attorney General asserts that disclosure of the surveillance information would endanger national security, the reviewing court should follow FISA.[65] These same circumstances, however, could also trigger a motion to dismiss under the state secret's privilege.[66]

---

[58] *Fazaga II*, 916 F.3d at 1231–32, 1238.

[59] *Id.*

[60] *Id.* at 1231.

[61] 50 U.S.C. § 1806(f) (2018). FISA states:

> Whenever any motion or request is made by an aggrieved person . . . 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 [court] . . . 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.

Id.

[62] *Id.*

[63] *See Fazaga II*, 916 F.3d at 1231–32 (holding that the text of FISA directly addresses the question previously answered by the common-law state secrets privilege). The government argued that absent a clear statement from Congress, principles of constitutional avoidance—the notion that courts should avoid interpreting statutes in a way that raises difficult constitutional issues—required the court to uphold the state secrets privilege. *Id.* at 1230; *see* Caleb Nelson, *Avoiding Constitutional Questions Versus Avoiding Unconstitutionality*, 128 HARV. L. REV. 331, 331 (2015) (defining constitutional avoidance). The court clarified that although the privilege has "constitutional overtones," it is a common-law evidentiary rule. *Fazaga II*, 916 F.3d at 1230.

[64] *Fazaga II*, 916 F.3d at 1232.

[65] *See* 50 U.S.C. § 1806(f); *Fazaga II*, 916 F.3d at 1232 (concluding that the nearly identical circumstances under which FISA and the state secrets privilege apply demonstrate the legislative intent to displace the use of the privilege in the context of electronic surveillance).

[66] *See* 50 U.S.C. § 1806(f); *Fazaga II*, 916 F.3d at 1232. Similar to the review procedure in FISA, the state secrets privilege is applicable whenever the head of the relevant governmental department asserts a formal claim of privilege in the name of national security. *See Fazaga II*, 916 F.3d at 1232 (comparing the concerns underlying the state secrets privilege with those underlying FISA).

The Ninth Circuit interpreted this overlap as a signal from Congress that courts should utilize FISA procedures in circumstances that would otherwise trigger the state secrets privilege.[67]

Second, looking to the rest of the statute and its legislative history, the Ninth Circuit concluded that Congress intended to create a comprehensive process for courts to evaluate government assertions of privilege over electronic surveillance for national security purposes.[68] The Ninth Circuit thus found no reason to restrict FISA's applicability to FISA claims.[69] For one, the statute was passed in the wake of a condemnatory Senate investigation into the executive branch's unauthorized surveillance activities.[70] The investigation exposed the executive branch's unlawful surveillance practices and concluded that the judiciary had failed to create a legal framework capable of protecting the constitutional rights of citizens.[71] Moreover, Congress has referred to FISA procedures, in combination with provisions of the Wire Tap Act and the Stored Communications Act, as the only lawful means of conducting electronic surveillance.[72] According to the Ninth Circuit, the language of, and legislative intent behind, the statute evidenced an attempt to create additional checks on executive power.[73]

---

[67] *See Fazaga II*, 916 F.3d at 1232 (explaining that FISA replaces the state secrets privilege because FISA requires *in camera* and *ex parte* review in the same circumstances that, were it not for FISA, would call for dismissal of the case under the state secrets privilege).

[68] *See id.* at 1234 (explaining that in the aftermath of the Senate investigation, Congress aimed to balance the often-times conflicting goals of national security and protecting individual rights against surveillance). The Ninth Circuit also pointed out the absurdity of allowing a court to review *in camera* and *ex parte* materials relating to a FISA claim, but not allowing the court to consider the same material as evidence in the same plaintiffs' non-FISA claims. *Id.* at 1238.

[69] *See id.* at 1236–37 (explaining that the language and purpose of FISA do not support the argument that the statute is applicable in only limited circumstances).

[70] *Id.* at 1233. The committee in charge of this investigation, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, was formed in 1975. *Id.* It is commonly referred to as the Church Committee. *Id.*

[71] *See id.* at 1233–34 (describing the findings and recommendations of the Church Committee following its investigation into the executive branch's surveillance tactics). The Church Committee attributed the executive branch's abuse of power to a failure to maintain the checks and balances designed by the Framers. *Id.* (quoting SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES & THE RIGHTS OF AMERICANS, S. REP. NO. 94–755, at 290 (1976)). It explained that because the law on electronic surveillance for national security purposes had developed entirely through case law, the doctrine was based on a small, unrepresentative sample of cases and failed to examine electronic surveillance intelligence holistically. *Id.* (quoting H. REP. NO. 95–183, pt. 1, at 21 (1978)).

[72] *Id.* at 1232–34 (citing 18 U.S.C. § 2511(2)(f) (2018) and S. REP. No. 95–604, pt. 1, at 7 (1978)); *see also* 18 U.S.C. § 2511 (1978) (establishing the Wiretap Act); 18 U.S.C. § 2701–2712 (1985) (establishing the Stored Communications Act). Both the Wiretap Act and the Stored Communications Act concern the disclosure of electronic communication information. 18 U.S.C. §§ 2511, 2701.

[73] *See Fazaga II*, 916 F.3d at 1234 (concluding that FISA aimed to create a fairer balance between national security and individual liberty concerns).

B. Protecting National Security and Personal Liberties

Although the government did not assert the state secrets privilege over the plaintiffs' Fourth Amendment or FISA claims, the district court dismissed the claims on state secrets grounds.[74] It reasoned that further litigation of the case would risk exposing information inextricably intertwined with privileged material, such as FBI sources, names of individuals under investigation, and counterterrorism strategies.[75]

In reversing the district court's judgement, the Ninth Circuit pointed out that the head of the relevant government department must formally claim the state secrets privilege and describe in detail why it is necessary.[76] The Ninth Circuit also reasoned that the district court's sweeping dismissal of the plaintiffs' claims contradicted the well-established principle that the state secrets privilege should be granted as infrequently as possible due to its severe curtailment of due process rights.[77]

The need to balance national security and individual rights—and the failure of the district court to do so—was essential to the Ninth Circuit's decision.[78] But the importance of invoking the state secrets privilege only when necessary has been argued before; it was fundamental to the assertion of privilege in *Reynolds* and courts have discussed it extensively in other state secrets cases, including the district court in *Fazaga I*.[79] For example, in determining whether to uphold the state secrets privilege, courts have consistently held that all of the evidence and circumstances of a case must be examined, including the importance of the information to the plaintiffs' claim and the nature of that

---

[74] *See* Fazaga v. Fed. Bureau Investigation (*Fazaga I*), 884 F. Supp. 2d 1022, 1045 (S.D. Cal. 2012) (concluding that the circumstances warranted terminating the case entirely rather than removing the specific evidence at issue).

[75] *Id.* at 1029.

[76] *Fazaga II*, 916 F.3d at 1228.

[77] *Id.*; *Fazaga I*, 884 F. Supp. 2d at 1045. *United States v. Reynolds* and subsequent cases discuss the importance of employing the state secrets privilege in limited circumstances. *See* 345 U.S. 1, 8 (1953) (explaining that too much investigation into a privilege claim would bring the very information that allegedly required protection to light, whereas too little investigation would result in unnecessary abuses of the privilege); *Fazaga I*, 884 F. Supp. 2d at 1041–42 (explaining that the decision as to whether to apply the state secrets privilege is ultimately left up to the courts, not the government department asserting it); *see, e.g.*, Mohamed v. Jeppesen, 614 F.3d 1070, 1081–82 (9th Cir. 2010) (discussing the need to defer to the executive branch on issues of foreign policy and to promote a fair adversarial process); El-Masri v. United States, 479 F.3d 296, 304–05 (4th Cir. 2007) (discussing the difficulty of balancing the role of the courts with that of the executive branch in the context of evaluating evidence); Wikimedia Found. v. Nat'l Sec. Agency, 335 F. Supp. 3d 772, 787 (D. Md. 2019) *appeal docketed*, No. 20-1191 (4th Cir. Feb. 18, 2020) (discussing courts' duty to defer to the executive branch without impetuously accepting claims of privilege).

[78] *See Fazaga II*, 916 F.3d at 1227–28 (discussing the importance of only invoking the state secrets privilege when necessary so as to protect meritorious claims from dismissal).

[79] *See supra* note 77 and accompanying text (providing examples of cases in which courts have emphasized the importance of using the state secrets privilege sparingly).

claim.[80] Likewise, courts agree that judicial deference to the executive on matters of foreign intelligence does not prevent a court from reviewing privileged information if it is not otherwise clear that the privilege claim is necessary.[81]

At the same time, the Ninth Circuit's decision recognized that in matters of national security, some degree of government secrecy—and thus some restriction on individual rights—is permissible.[82] The Ninth Circuit explained that although courts should not dismiss plaintiffs' claims outright on state secrets grounds, the nature of the information at stake may still prevent plaintiffs from realizing their normal due process rights.[83] Thus, FISA does not prevent the government from withholding discoverable information by revoking the state secrets privilege.[84] On the contrary, it codifies the privilege and sets forth a specific procedure for its application.[85]

III. CAREFUL BUT MEANINGFUL JUDICIAL REVIEW

The Supreme Court has made it clear that conducting electronic surveillance against United States citizens without judicial approval is an unreasonable exercise of executive power, regardless of the circumstances.[86] Still, most recent presidents have justified the use of electronic surveillance by asserting their power and responsibility to protect national security.[87] In the absence of

---

[80] *See Reynolds*, 345 U.S. at 10–11 (noting the relevance of the fact that the claim pertained to national defense efforts, specifically air power, and that the plaintiffs could likely litigate their claims without the information at issue); Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998) (explaining that a court should review claims of privilege in light of the case's particular circumstances).

[81] *See Reynolds*, 345 U.S. at 10 (noting that a court must be satisfied that the materials at issue present a reasonable danger of exposing secret information related to national security if the court is to employ the state secrets privilege); *El-Masri*, 479 F.3d at 305 (explaining that a court may conduct an *in camera* review of the allegedly privileged information if doing so is necessary to conclude that the *Reynolds* standard is met); Sterling v. Tenet, 416 F.3d 338, 345 (4th Cir. 2005) (noting that there will be instances in which a court reviews allegedly privileged information *in camera*).

[82] *See Fazaga II*, 916 F.3d at 1226 (stating that the FISA procedure will restrict the rights normally afforded to plaintiffs in court and that the state secrets privilege developed as a way to protect essential national security interests).

[83] *Id.*

[84] *See id.* at 1231–32 (explaining the plain meaning of FISA's language and the significance of its applicability in circumstances that would otherwise call for application of the state secrets privilege).

[85] *See id.* at 1232 (explaining that FISA reflects Congress's intent to formalize a procedure by which courts review electronic surveillance material when it relates to national security, thus codifying the state secrets privilege for matters related to FISA).

[86] *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 320 (1972) (explaining that although the President's contentions about the importance of certain information to the nation's security could not be dismissed lightly, the executive branch nevertheless must abide by Fourth Amendment standards).

[87] *See* U.S. CONST. art. II, § 1 (requiring that the President take an oath to protect and defend the Constitution); *Keith*, 407 U.S. at 310 (discussing the use of electronic surveillance for constitutional purposes by presidents throughout history); Nathan Alexander Sales, Article, *Secrecy and National Security Investigations*, 58 ALA. L. REV. 811, 839 (2007) (noting that various presidents have authorized illegal wiretaps in the name of national security).

adequate judicial or legislative oversight, this power has been abused.[88] Before the Supreme Court's 1972 decision in *United States v. U.S. District Court* (*Keith*), for example, the executive branch monitored thousands of innocent citizens for unusually long periods of time and used covert surveillance to track civil rights activists, pro-Communist groups, and other persons of political interest—all without a warrant.[89] And, before the enactment of the Foreign Intelligence Surveillance Act (FISA), the government secretly collected and used information about citizens' political activities, associations, and personal lives.[90] In his concurring opinion in *Keith*, Justice Douglas stated that these practices are an unsurprising consequence of unbridled executive discretion.[91] The majority agreed, declaring that legislative guidance and judicial review of government decisions are essential to protecting individual freedoms such as privacy.[92]

The Southern District of California's approach in 2012 in *Fazaga v. Federal Bureau of Investigation* (*Fazaga I*) exemplifies the *Keith* Court's concerns.[93] The district court erred in dismissing all of the plaintiffs' claims on state secrets grounds, despite the government only asserting the privilege over the religion claims.[94] Likewise, the court improperly disregarded the review

---

[88] *See Keith*, 407 U.S. at 325–26 (Douglas, J., concurring) (discussing the executive branch's abuse of its ability to conduct warrantless surveillance and providing examples of government activity leading up to the *Keith* decision); Sales, *supra* note 87, at 839 (discussing the executive branch's surveillance activity in the 1960s and 1970s).

[89] *See Keith*, 407 U.S. at 325–26 (Douglas, J., concurring) (explaining the defendants' surveillance activity and providing examples of instances in which their tactics appeared extreme); Sales, *supra* note 87, at 839 (providing examples of the kinds of surveillance the executive branch conducted without judicial oversight). *See generally* 50 U.S.C. § 1801–1813 (2018). For example, the FBI infamously surveilled Martin Luther King Jr. during this period and later used the information to blackmail him. Sales, *supra* note 87, at 839. King was first investigated in 1955 after organizing a 385-day bus boycott in Montgomery, Alabama. Ryan Sit, *Here's What the FBI Had on Martin Luther King Jr.*, NEWSWEEK (Jan. 15, 2018), https://www.newsweek.com/fbi-martin-luther-king-jr-surveillence-wiretap-report-j-edgar-hoover-780630 [https://perma.cc/E8KC-4QAE]. By 1965 the Bureau had tapped King's phone calls and bugged his house, office, and hotel rooms. *Id.*

[90] Fazaga v. Fed. Bureau Investigation (*Fazaga II*), 916 F.3d 1202, 1233 (2019) (quoting SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES & THE RIGHTS OF AMERICANS, S. REP. NO. 94–755, at 290 (1976)).

[91] *See Keith*, 407 U.S. at 326–27 (Douglas, J., concurring) (noting that the government's willingness to invade individuals' privacy in the name of security is the very reason that the Constitution requires the executive branch to obtain a warrant before conducting domestic surveillance).

[92] *See id*. at 316–18 (explaining that because individual rights are protected by a separation of powers among the three branches, the executive branch should not judge its own decisions).

[93] *See infra* notes 94–96 and accompanying text (explaining the district court's decisions in *Fazaga I* and their potential consequences had they been upheld).

[94] *Fazaga II*, 916 F.3d at 1228; *see* Fazaga v. Fed. Bureau Investigation (*Fazaga I*), 884 F. Supp. 2d 1022, 1042, 1045 (S.D. Cal. 2012) (concluding that the information collected throughout Operation Flex would pose a great public safety risk if disclosed and thus that all claims dependent on this evidence be dismissed).

procedure that Congress designed for cases like *Fazaga I*.[95] Consequently, if the district court had its way, the executive branch would be able to conduct certain electronic surveillance activities without having to follow the legislature's plan or being subject to the court's review.[96]

In contrast, the Ninth Circuit in *Fazaga v. Federal Bureau of Investigation* (*Fazaga II*) concluded that Congress and the judiciary may check the executive's use of electronic surveillance without compromising the essential role of executive power in matters of national security.[97] First, FISA allows the government to conduct electronic surveillance so long as it has some measurable relation to foreign intelligence.[98] When determining whether such a relation exists, courts should defer to the relevant national security official.[99] This standard, which would apply with or without FISA's displacement of the state secrets privilege, preserves the executive branch's authority over the use of electronic surveillance.[100] Second, when parties request electronic surveillance information related to national security, FISA's review procedure prevents courts from disclosing any purportedly privileged information unless it is es-

---

[95] *Fazaga II*, 916 F.3d at 1230; *see Fazaga I*, 884 F. Supp. 2d at 1038 (finding no reason to support "an expansive application of FISA").

[96] *See Fazaga II*, 916 F.3d at 1228, 1234 (discussing the district court's dismissal of all the plaintiffs' claims and concluding that FISA represents an effort to review the surveillance activities of the executive branch). *See generally Fazaga I*, 884 F. Supp. 2d at 1029.

[97] *See Fazaga II*, 916 F.3d at 1232 (explaining that although the FISA procedure modifies the review process under the state secrets privilege, FISA is also concerned with threats to national security).

[98] *See* 50 U.S.C. § 1804(a) (providing that the government is authorized to use electronic surveillance so long as foreign intelligence is a significant purpose of the surveillance); *In re* Sealed Case, 310 F.3d 717, 735–36 (Foreign Int. Surv. Ct. Rev. 2002) (holding that the significant purpose standard is met so long as the government realistically shows that it is dealing with foreign intelligence rather than criminal prosecution); Dvorske, *supra* note 31, § 3b (explaining the circumstances under which a judge should issue an order for the use of electronic surveillance). The significant purpose standard is lower than the standard that traditionally must be met to obtain a warrant, which requires a showing that the investigation is the primary purpose of the surveillance. *See* United States v. Abu-Jihaad, 630 F.3d 102, 120 (2d Cir. 2010) (holding that if it has probable cause, the government is able to obtain a warrant for any good-faith pursuit); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (holding that electronic surveillance may be allowed on less than the traditional probable cause standard because of the Fourth Amendment protections built into FISA). Previously, FISA required the government to show that the primary purpose of the surveillance was foreign intelligence. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1805 (amended 2001). Congress amended this provision following the September 11th attacks through the Patriot Act, which generally expanded the power of the executive branch to conduct surveillance for the purpose of preventing terrorist attacks. *See* Dvorske, *supra* note 31, at 385 (discussing the amendment of FISA through the USA PATRIOT Act and the Fourth Amendment probable cause concerns that the amendment brought about).

[99] *See In re Sealed Case*, 310 F.3d at 736 (stating that the national security official in charge of the matter is meant to judge the government's purpose in using electronic surveillance, rather than the FISA court).

[100] *See id.* (noting that the Attorney General has full authority to decide whether to authorize an investigation).

sential to determining the legality of the surveillance.[101] As of October 2019, no court of appeals has made such a disclosure.[102] The difference between the procedures provided in FISA and the dismissal remedy under the state secrets privilege is, therefore, minimal— FISA calls upon judges to review, *in camera* and *ex parte*, the material at issue, whereas the state secrets privilege permits courts to exercise this review only when absolutely necessary.[103] Thus, neither procedure allows for the disclosure of privileged information to the plaintiffs.[104] FISA merely prevents the executive branch from escaping review altogether.[105]

As the capacity for covert electronic surveillance expands, the executive branch continues to face scrutiny for its broad use of electronic surveillance domestically and abroad.[106] Without a system of formal review in place, the ease with which the executive branch may employ unwarranted surveillance technology and infringe on individuals' privacy will continue to grow.[107] Although the use of electronic surveillance remains essential to the executive branch for national security purposes, technologies such as facial recognition, computer hacking, and internet surveillance present new, unsanctioned ways to intrude on individual privacy.[108]

---

[101] 50 U.S.C. § 1806(f).

[102] *See* KRIS & WILSON, *supra* note 26, § 31:3 (reviewing the history of the FISA review procedure and the outcomes of FISA litigation). In *Keith*, the Supreme Court rejected the argument that receiving judicial approval prior to conducting any electronic surveillance would threaten the secrecy necessary for a successful intelligence operation. 407 U.S. at 320–21. The Court noted that judges have historically dealt carefully with confidential information and could be relied upon to respect the secrecy required by law. *Id.*

[103] *See* 50 U.S.C. § 1806(f) (outlining FISA's review procedure); United States v. Reynolds, 345 U.S. 1, 8 (1953) (noting that a court must find that the materials at issue present a reasonable danger of exposing secret information related to national security if it is to employ the state secrets privilege).

[104] *See* KRIS & WILSON, *supra* note 26, § 31:3 (describing the legislative history of FISA and analyzing the importance of various FISA cases).

[105] *See* 50 U.S.C. § 1806(f) (providing a review procedure by which the judiciary can ensure the validity of the government's claim).

[106] *See* Mark D. Young, *Electronic Surveillance in an Era of Modern Technology and Evolving Threats to National Security*, 22 STAN. L. & POL'Y REV. 11, 11–12 (2011) (discussing the rise of the internet, electronic mail, data sharing, and other technology, all of which provide access to personal information); Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/NGV2-DW7P], (reporting that the National Security Administration had been collecting the telephone records of millions of Americans); Sheila A. Millar, *Electronic Surveillance and Monitoring*, KELLER & HECKMAN LLP (Nov. 01, 2004), https://www.khlaw.com/1225 [https://perma.cc/ZC76-RPL4] (discussing the increase in U.S. surveillance activities after September 11th and finding that governments across the world have generally expanded the use of surveillance tactics over time).

[107] *See* Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 298 (1999) (discussing the increasing ability of law enforcement to conduct electronic surveillance); Sengupta, *supra* note 3 (reporting large increases in the City of Oakland's spending on the collection of surveillance data and technological equipment).

[108] *See* Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and* Kyllo*: How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L.

In order to prevent national security interests from smothering individuals' right to be free from arbitrary privacy invasions, Congress must regulate the implementation of this new technology, and the judiciary must have the power to review executive compliance.[109] By holding that FISA preempts the state secrets privilege, the Ninth Circuit ventured to protect the role of all three branches in complex decisions about the expanding use of electronic surveillance.[110] In doing so, the Ninth Circuit kept both national security and individual liberty in mind.[111]

CONCLUSION

Courts struggle to balance protecting individual liberty with legitimate national security concerns. But the district court in *Fazaga v. Federal Bureau of Investigation* did no balancing; it prioritized the government's potential national security interests over all of the plaintiffs' potentially meritorious claims. Recognizing this failure, the Ninth Circuit replaced the state secrets privileges with the procedures Congress enacted in the Federal Intelligence Surveillance Act. By preserving *in camera* and *ex parte* review of information retrieved through electronic surveillance for foreign intelligence purposes, the Ninth Circuit appropriately balanced deference to the executive branch against the preservation of private citizens' individual liberties. *Fazaga II* did not uproot notions of executive primacy over the other branches when dealing with issues of national security. Instead, it reinforced a system that prioritizes the executive's judgment while maintaining checks and balances against abuse of its power.

JESSLIN WOOLIVER

Preferred citation: Jesslin Wooliver, Comment, *Want to Know a Secret . . .? Electronic Surveillance, National Security, and the Role of the Foreign Intelligence Surveillance Act*, 61 B.C. L. REV. E. SUPP. II.-393 (2020), http://lawdigitalcommons.bc.edu/bclr/vol61/iss9/35/

REV. 719, 755–56, 758, 762–63 (2015) (discussing the growing use of online communication and data collection and the dangers associated with it); Young, *supra* note 106, at 11 (listing new technological advances that affect national security); Milligan, *supra* note 107, at 303–04 (discussing facial recognition technology and its effect on electronic surveillance); *see also* John L. Potapchuk, Note, *A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act*, 57 B.C. L. REV. 1403, 1403 (2016) (arguing that federal courts have the authority to compel third parties to provide government authorities with consumer data).

[109] *See Keith*, 407 U.S. at 316–17 (concluding that in the absence of judicial review, the executive branch is pressured to pursue its prosecutorial duty without consideration of individual rights).

[110] *See Fazaga II*, 916 F.3d at 1233–34 (concluding that FISA grants all three branches a role in governing the executive's use of electronic surveillance while ensuring that the executive branch's concerns about national security are safeguarded).

[111] *See infra* notes 100–104 and accompanying text (discussing the ways in which FISA protects the executive branch's authority over matters of foreign intelligence and national security without neglecting the role of the judiciary in overseeing its activity). *See generally Fazaga II*, 916 F.3d at 1232.