

November 2020

## Fazaga v. FBI: Putting the Force Back in the Foreign Intelligence Surveillance Act

Christina Ferreiro

Follow this and additional works at: <https://repository.law.miami.edu/umrsjlr>



Part of the [Law and Race Commons](#), and the [Law and Society Commons](#)

---

### Recommended Citation

Christina Ferreiro, *Fazaga v. FBI: Putting the Force Back in the Foreign Intelligence Surveillance Act*, 11 U. Miami Race & Soc. Just. L. Rev. 76 (2020)

Available at: <https://repository.law.miami.edu/umrsjlr/vol11/iss1/6>

This Note is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Race & Social Justice Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact [library@law.miami.edu](mailto:library@law.miami.edu).

# Fazaga v. FBI: Putting the Force Back in the Foreign Intelligence Surveillance Act

Christina Ferreiro\*

I.	INTRODUCTION .....	78
II.	THE FOREIGN INTELLIGENCE SURVEILLANCE ACT.....	79
	<i>a. Pre-FISA: The Judicial Response to Electronic Surveillance ...</i>	80
	<i>b. FISA: The Legislative Response to Executive Abuse.....</i>	82
	<i>c. FISA in Operation: Legislative Structure and Protections.....</i>	83
	i. Procedural Safeguards.....	83
	ii. Constitutional Protections .....	85
III.	STATE SECRETS .....	86
IV.	FAZAGA V. FBI.....	89
V.	ANALYSIS .....	92
	<i>a. The Court Justifiably Applied Careful Fourth Amendment</i>	
	<i>Analysis.....</i>	92
	i. The Reasonable Expectation of Privacy Analysis Under	
	FISA is the Same as Under the Fourth Amendment .....	93
	ii. Plaintiffs Expectations of Privacy are Greater in	
	Religious Spaces .....	94
	<i>b. The Court Reinforced Separation of Powers Principles in</i>	
	<i>Holding FISA Procedures Overruled the State' Secrets</i>	
	<i>Dismissal Remedy.....</i>	98
	i. The Court Correctly Affirmed that Reynolds is a Rule of	
	Evidence, Not a Constitutional Construction for Unitary	
	Executive Power .....	99
	ii. The Court Accepted Congress's Invitation to Provide a	

---

\* Juris Doctor Candidate, 2021, at the University of Miami. As a Miami Public Interest Scholar, I have spent my law school career devoted to issues surrounding the protection of civil liberties. I am eternally grateful to the many professors at the University of Miami who have encouraged me to think critically about the law, the constitution, and policy. I am especially thankful to my fellow classmates and friends who challenge me and support me simultaneously. Most of all, I am beyond grateful for my parents, Ana and Juan Carlos, for providing me with unconditional support and teaching me the value of hard work. Finally, thank you to the team of brilliant minds that make up the University of Miami Race and Social Justice Law Review.

Constitutionally Granted Joint Check on the President ..... 100  
iii. The Court Fulfilled the Constitutional Duties of the  
Judiciary Branch ..... 102  
VI. CONCLUSION..... 103

## I. INTRODUCTION

“We needed a way to keep an eye on the American citizens without them knowing. It was imperative, for their own safety of course.” – President Richard Nixon (1978)

Sheikh Yassir Fazaga, Ali Uddin Malik, and Yasser AbdelRahim resided in Southern California.<sup>1</sup> They spent their days working, spending time with their families, and attending mosque.<sup>2</sup> In 2006, although they did not know it at the time, nor could they, their lives changed when their daily activities began being surveilled by the Federal Bureau of Investigations (“FBI”) without their knowledge or consent.<sup>3</sup> Under a dragnet surveillance program titled “Operation Flex,” the FBI targeted and surveilled hundreds of Muslims in the orange county area to obtain as much information as possible.<sup>4</sup> Fazaga, Malik, and AbdelRahim represent a class of Muslims whose constitutional rights to freedom of religion and privacy were invaded for no reason other than their Muslim religion.<sup>5</sup> Unfortunately, in the wake of the tragic 9/11 attacks, their story and the substantial invasion of their rights is all too common for Muslims across America. The relationship between Muslim-Americans and law enforcement has been one of tension for several years, as law enforcement’s attempts to build trust with Muslim communities in order to rely on community members to provide essential information on terrorist activities are undermined by the invasion of substantial rights of the very same Muslims they pretend to be in harmony with.<sup>6</sup> These methods of depriving Muslims of constitutionally protected rights have been numerous and far-reaching, ranging from the use of evidence

---

<sup>1</sup> First Amended Complaint at 21-25; *Fazaga v. Fed. Bureau of Investigation*, 916 F.3d 1202, 21-25 (9th Cir. 2019) (No. SA-CV-11-00301) [hereinafter First Amended Complaint].

<sup>2</sup> *Id.*

<sup>3</sup> *Id.* at 15-18.

<sup>4</sup> *Id.* at 1-2, 27.

<sup>5</sup> *Id.* at 2.

<sup>6</sup> See generally Bryan Tau, *What is FISA? The Surveillance Law Behind the Memo Explained*, THE WALL STREET JOURNAL (Feb. 2, 2018); See Human Rights Institute, *Illusions of Justice: Human Rights Abuses in US Terrorism Prosecutions*, at 5 (July 2014). [hereinafter *Illusions of Justice*] (discussing Ahmed Omar Abu Ali, a US citizen, who was swept up in a mass arrest campaign in Saudi Arabia in 2003. Ali was whipped, denied food, and threatened with amputation before he succumbed to his interrogators and gave a false confession. At his trial in the United States, the judge ignored his claims of torture and admitted his confession into evidence. He was convicted and is serving a life sentence in solitary confinement in a supermax prison in Colorado).

obtained by coercion<sup>7</sup> to inhumane detention conditions.<sup>8</sup> Since the attacks of 9/11, the use of electronic surveillance in particular has been more frequent, and nearly every branch of government has relaxed the conditions of using electronic surveillance to spy on those suspected of terrorism activities.<sup>9</sup>

This note uses the Ninth Circuit's decision in *Fazaga v. FBI* to illustrate how the Foreign Intelligence Surveillance Act can be used as a tool to the benefit of, rather than merely to the detriment of, Muslims in America in order to protect their constitutional right to be free of invasions of privacy on the basis of their religion. Part II of this note discusses the history of the Foreign Intelligence Surveillance Act ("FISA"), from the historically documented executive abuse of suspicionless electronic surveillance, to the creation and operation of FISA. Part III examines the history of the state secrets privilege, often used as a cloak for the governments unconstitutional and abusive investigation tactics under the guise of national security. Part IV of this note summarizes the facts and shocking details of the case, *Fazaga v. FBI*, paying particular attention to the egregious manner in which the FBI's undercover informant intruded on the privacy of Muslim individuals. Part V provides an in-depth analysis of the Ninth Circuit's holding in *Fazaga v. FBI*. Part V.A analyzes the Ninth Circuit's decision with regard to the substantive FISA claims, noting the court correctly applied the reasonable expectation of privacy test to *Fazaga's* claims. Finally, Part V.B argues the Ninth Circuit's holding that FISA displaces the state secrets privilege and thus plaintiff's claims could proceed under the procedures set forth in FISA without offending constitutional principles of separation of powers.

## II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

"Americans fought a revolution in part over the right to be free from unreasonable searches – to ensure that our government could not come

---

<sup>7</sup> See *Illusions of Justice*, *supra* note 6, at 7 (discussing Ahmed Omar Abu Ali, a US citizen, who was swept up in a mass arrest campaign in Saudi Arabia in 2003. Ali was whipped, denied food, and threatened with amputation before he succumbed to his interrogators and gave a false confession. At his trial in the United States, the judge ignored his claims of torture and admitted his confession into evidence. He was convicted and is serving a life sentence in solitary confinement in a supermax prison in Colorado).

<sup>8</sup> *Id.* at 7 (discussing Uzair Paracha, who was held in solitary confinement for almost two years before he was convicted on material support to terrorist activities charges. Nine months after he was convicted, he spent another 9 months in solitary, unable to say anything to anyone except the security guards, largely begging them to turn the lights off or ask for basic necessities).

<sup>9</sup> *Id.* at 59.

knocking in the middle of the night for no reason. We need to find a way forward to make sure we can stop terrorists with protecting the privacy and liberty of innocent Americans.” – Barack Obama (2006)

*a. Pre-FISA: The Judicial Response to Electronic Surveillance*

The Supreme Court first addressed the federal government’s use of warrantless electronic surveillance in *Olmstead v. United States*,<sup>10</sup> in which it held electronic surveillance through wiretapping does not require a warrant under the Fourth Amendment because such activity does not amount to a search or seizure within the Fourth Amendment.<sup>11</sup> However, years later in *Katz v. United States*,<sup>12</sup> the Supreme Court changed positions and held that because “the Fourth Amendment protects people, not places,”<sup>13</sup> the wiretapping of a phone booth constitutes a search and seizure within the meaning of the Fourth Amendment, and is therefore subject to the Fourth Amendment’s warrant requirement.<sup>14</sup> Since then, the Court has implemented a “reasonable expectation of privacy” test pronounced in Justice Harlan’s concurring opinion in *Katz* to evaluate Fourth Amendment violations.<sup>15</sup> *Katz*, however, was a domestic case involving electronic surveillance in the pursuit of criminal prosecution, the Supreme Court did not decide whether the executive may conduct warrantless electronic surveillance for the purpose of national security.<sup>16</sup>

The Supreme Court addressed the executive’s constitutional authority to conduct warrantless electronic surveillance of domestic threats to national security in *United States vs. United States District Court (Keith)*.<sup>17</sup> In *Keith*, the defendant planted an overnight bomb meant to destroy the property of a local C.I.A. office in protest to the C.I.A. presence in Ann

---

<sup>10</sup> *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967).

<sup>11</sup> *Id.* at 466.

<sup>12</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>13</sup> *Id.* at 351.

<sup>14</sup> *Id.* at 359.

<sup>15</sup> *Id.* at 360-61; *See also* Scott J. Glick, *FISA’s Significant Purpose Requirement and the Government’s Ability to Protect National Security*, 1 HARVARD NAT’L SECURITY L. REV., 87, 94 (May 30, 2010).

<sup>16</sup> *Katz*, 389 U.S. at 358 n.23 (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”)

<sup>17</sup> *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 314-22 (1972). The case is known as the *Keith* case because it arose out of a writ of mandamus against the Honorable Judge Damon Keith, United States District Court Judge, who ordered the government to disclose wiretapping information.

Arbor, Michigan.<sup>18</sup> The defendant attempted to compel the government to produce evidence pertaining to information gathered by electronic surveillance.<sup>19</sup> The government refused to disclose the surveillance evidence, claiming the surveillance was a reasonable exercise of the President's inherent authority to protect national security, and that disclosure would threaten national security.<sup>20</sup> The Court, while recognizing the president's duty to protect the nation from threats to national security, nonetheless held that the Fourth Amendment requires the president to obtain a warrant before engaging in electronic surveillance for domestic security purposes.<sup>21</sup>

While the Court in *Keith* limited its ruling to domestic surveillance, expressly reserving the question of the president's authority in cases of foreign powers or their agents,<sup>22</sup> the decision was highly suggestive as to Congress's powers to proscribe procedures for national security surveillance that comply with the Fourth Amendment.<sup>23</sup> Significantly, the Court acknowledged that in the case of intelligence gathering, [d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of the citizen rights deserving protection.<sup>24</sup>

*Keith* was significant in both recognizing congress's authority to enact specific procedures for intelligence gathering, and also noting that the procedures proscribed may very well differ from the standards set by the Fourth Amendment when the pursuit is intelligence gathering.<sup>25</sup> *Keith* created a circuit split among courts that accepted an implicit exception to the warrant requirement where the national security threat was a foreign power, and others that would not recognize an exception for foreign security threats.<sup>26</sup> Subsequent historical events involving the executive branch's abuse of power in the name of national security compelled

---

<sup>18</sup> *Id.* at 299.

<sup>19</sup> *Id.* at 299-300.

<sup>20</sup> *Id.* at 301.

<sup>21</sup> *Id.* at 320-22. ("We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment.")

<sup>22</sup> *Id.* at 321-22.

<sup>23</sup> *Id.* at 322.

<sup>24</sup> *Id.* at 322-23.

<sup>25</sup> See Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting Civil Liberties That Make Defense of Our Nation Worthwhile*, 35 SW. U. L. REV. 361, 366 (2006).

<sup>26</sup> See Robert A. Dawson, *Shifting the Balance: The D.C. Circuit and the Foreign Intelligence Surveillance Act of 1978*, 61 GEO. WASH. L. REV. 1380, 1385 (June 1993).

Congress to heed the Supreme Court's advice in *Keith* and legislate in the field of intelligence gathering.<sup>27</sup>

*b. FISA: The Legislative Response to Executive Abuse*

It is 1973 in Washington D.C., the political parties have set aside their differences and all three branches of government have banded together as a result of one of the most salient and atrocious abuses of power America has suffered in recent history: Watergate.<sup>28</sup> American Presidents have historically claimed the ability to conduct warrantless national security surveillance as ancillary to their duty to protect from national security threats.<sup>29</sup> The other branches held the belief that the executive branch was overreaching its constitutionally granted powers and infringing on civil liberties in the process.<sup>30</sup>

This tension came to a head when President Nixon's scandalous use of electronic surveillance to spy on his political party opponents became public.<sup>31</sup> The legislature soon realized that Nixon used the guise of national security to justify illegally spying on those lawfully engaged in political dissent.<sup>32</sup> In response to President Nixon's abuse of warrantless electronic surveillance, an investigation was launched, known as the "Church Committee" to discover what other abuses had occurred as a result of unchecked executive power under the guise of national security.<sup>33</sup>

The Church Committee uncovered a startling history of government exploiting electronic surveillance since the 1930s, the targets of which ranged from congressmen, White House advisors, anti-war protest groups, and others who posed no actual threat to national security.<sup>34</sup> The two-year long investigation by the Church Committee revealed that President Eisenhower authorized the FBI to conduct domestic electronic surveillance on political opponents, including Martin Luther King Jr.'s Southern Christian Leadership Conference.<sup>35</sup> The Church Committee

---

<sup>27</sup> *Id.* at 1385-88.

<sup>28</sup> Carl Bernstein & Bob Woodward, *FBI Finds Nixon Aides Sabotaged Democrats*, WASH. POST (Oct. 10, 1972), <http://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/101072-1.htm>.

<sup>29</sup> See Dawson, *supra* note 26, at 1382.

<sup>30</sup> *Id.*

<sup>31</sup> Elizabeth Goitein & Faiza Patel, *What Went Wrong With The FISA Court*, 14, BRENNAN CENTER FOR JUSTICE, (2015).

<sup>32</sup> Dawson, *supra* note 26, at 1386.

<sup>33</sup> See Whilt, *supra* note 25, at 385.

<sup>34</sup> *Id.*; see also S. REP. NO. 95-604, at 7, (noting that while a number of illegal or improper national security taps and bugs conducted during the Nixon administration may have exceeded those in previous administrations, the surveillance was regrettably by no means atypical).

<sup>35</sup> Goitein & Patel, *supra* note 31, at 13.



found that every executive since Franklin D. Roosevelt had claimed the power to authorize warrantless electronic surveillance and abused that power.<sup>36</sup> Congress became especially concerned with the potential stifling of constitutionally protected speech in the form of political dissent.<sup>37</sup> The unsettling discovery of executive abuse motivated the executive branch and congress to create legislation that would safeguard against overreaching executive power in the form of warrantless electronic surveillance.<sup>38</sup> In 1978, as a reaction to the Church Committee's discoveries, congress enacted FISA.<sup>39</sup>

*c. FISA in Operation: Legislative Structure and Protections*

*i. Procedural Safeguards*

FISA establishes a statutory procedure that allows the government to conduct electronic surveillance<sup>40</sup> by first obtaining judicial approval.<sup>41</sup> FISA mandates that before a government agency conducts electronic surveillance, the government agency must obtain a particular warrant ("FISA warrant") by a special tribunal body, the Foreign Intelligence

---

<sup>36</sup> See STAFF OF S. COMM. ON INTELLIGENCE AND THE RIGHTS OF AMERICAS, 95TH CONG., FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (Comm. Print 1978). [hereinafter SENATE JUDICIARY REPORT].

<sup>37</sup> *Id.* at 3909-10. ("Also formidable-although incalculable-is the 'chilling effect' which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of the surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with government activities which effectively inhibit the exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy, within lawful limits, without having to sacrifice the expectation of privacy that they rightfully hold. Arbitrary or uncontrolled use of warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.")

<sup>38</sup> Goitein & Patel, *supra* note 31, at 14.

<sup>39</sup> See Dawson, *supra* note 26, at 1386. See also SENATE JUDICIARY REPORT, *supra* note 36, at 3908 ("the need for such statutory safeguards has become apparent in recent years. This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the nation of national security has been seriously abused.").

<sup>40</sup> See 50 U.S.C. § 1801(f). FISA defines electronic surveillance under four categories; (1) acquisition of wire or radio communications that intentionally targets a particular known United States person who is in the United States; (2) acquisition of wire communication to or from a person in the united states, without consent of any party, if the acquisition occurs in the united states; (3) the intentional acquisition of radio communication if both the sender and recipients are in the United States; and (4) the installation of electronic, mechanical, or other surveillance device in the United States other than from a wire or radio.

<sup>41</sup> See Dawson, *supra* note 26, at 1389.

Surveillance Court (“FISC”).<sup>42</sup> First, the government files a detailed application to FISC requesting authorization for electronic surveillance of a facility or place.<sup>43</sup> The application must contain a sworn statement by a federal officer and be approved by the attorney general.<sup>44</sup> The application must also include “the identity or description of the target of surveillance,<sup>45</sup> a statement of facts that justify the belief that the target is an agent of a foreign power,<sup>46</sup> a statement of the proposed minimization procedures,<sup>47</sup> a description of the “nature of the information sought and the type of communications or activities to be subjected to the surveillance,”<sup>48</sup> and a certification that the purpose of the surveillance is to obtain foreign intelligence information that cannot “reasonably be obtained by normal investigative techniques,”<sup>49</sup> among other things.

The FISA court must then find that the application does indeed contain the above requirements,<sup>50</sup> and enter an order describing the identity of the target, the nature and location of the sites where the surveillance is to be conducted, the type of information sought, the means to be employed, and the period of time for which the surveillance is approved.<sup>51</sup> Importantly, for the application to be approved, the government must show *probable cause* to believe the target is a foreign power or agent of a foreign power, and that the facility or place to be surveilled is used or about to be used by the target.<sup>52</sup> By requiring the government to elaborate their suspicions with specific details, FISA places strict limits on the executive’s ability to conduct electronic surveillance in an effort to suppress lawful political dissent.<sup>53</sup>

Congress also built in a course of redress whenever electronic surveillance for the purpose of intelligence gathering is conducted without

---

<sup>42</sup> See Glick, *supra* note 15, at 93.

<sup>43</sup> See Director of National Intelligence, *The FISA Amendments Act: Q&A 1* (Apr. 18, 2017), <https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Public%20ation.pdf>.

<sup>44</sup> 50 U.S.C. § 1804(a) (“Each application for an order approving electronic surveillance under this chapter shall be made by a Federal officer in writing upon oath or affirmation to a [FISA court] judge. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this chapter.”)

<sup>45</sup> 50 U.S.C. § 1804(a)(2).

<sup>46</sup> 50 U.S.C. § 1804(a)(3).

<sup>47</sup> 50 U.S.C. § 1804(a)(4).

<sup>48</sup> 50 U.S.C. § 1804(a)(5).

<sup>49</sup> 50 U.S.C. § 1804(a)(6).

<sup>50</sup> 50 U.S.C. § 1805(a).

<sup>51</sup> 50 U.S.C. § 1804(c)(1).

<sup>52</sup> 50 U.S.C. § 1805(a)(4).

<sup>53</sup> Goitein & Patel, *supra* note 31, at 14.

a FISA warrant.<sup>54</sup> FISA provides that a person who “engages in electronic surveillance under color of law except as authorized by [FISA, the Wiretap Act, the Stored Communications Act, or the pen register statute] or any express statutory authorization” is guilty of a criminal offense.<sup>55</sup> FISA also provides for a private right of action for an aggrieved person<sup>56</sup> who has been subjected to surveillance against the person who committed the surveillance.<sup>57</sup> Finally, and most significantly for this note, FISA allows for *in camera* and *ex parte* review by a district court of “the application, order or other materials relation to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted” under statutorily defined circumstances.<sup>58</sup>

## ii. Constitutional Protections

The purpose of FISA was to strike a balance in which the executive branch could conduct legitimate foreign intelligence surveillance without abridging the right to individual privacy and civil liberties guaranteed by the constitution.<sup>59</sup> FISA warrants, while providing significantly diminished protections than traditional law enforcement warrants,<sup>60</sup> are imperative to retaining any meaningful First and Fourth Amendment rights. This is because in times of national security crises, the government looks most suspiciously to those who exercise their First Amendment rights to political speech and exercise of religion.<sup>61</sup> The Supreme Court noted in *Keith* that national security cases reveal an extraordinary merging of First and Fourth Amendment rights because although “the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech.”<sup>62</sup>

Indeed, there is a history of the Federal Government sacrificing individual liberties in the name of national security whenever they

---

<sup>54</sup> See *infra* notes 55-58 and accompanying text.

<sup>55</sup> 50 U.S.C. § 1809(a).

<sup>56</sup> 50 U.S.C. § 1801(k) (defining “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.”).

<sup>57</sup> 50 U.S.C. § 1810 (providing “an aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation.”)

<sup>58</sup> 50 U.S.C. § 1806(f).

<sup>59</sup> See Dawson, *supra* note 26, at 1386-87.

<sup>60</sup> For a comparison of protections and procedures offered by Title III warrants and FISA warrants, see Whilt, *supra* note 25.

<sup>61</sup> See Robert M. Chesney, *Civil Liberties and the Terrorism Prevention Paradigm: The Guilty By Association Critique*, 101 MICHIGAN L. REV. 1408, 1418 (2003).

<sup>62</sup> United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 313-14 (1972).

perceive a “threat” among a particular group.<sup>63</sup> In the post-9/11 era, the focus has shifted to Muslim Americans exercising their constitutionally protected freedom of religion guaranteed by the First Amendment.<sup>64</sup> For example, the FBI has expended considerable energy on creating demographic profiles to map the racial, ethnic and religious make up of communities in order to pin point their investigative sights.<sup>65</sup> After targeting these groups solely based on unconstitutional religious profiling,<sup>66</sup> the FBI infiltrates Muslim communities by sending undercover informants, often posed as newcomers seeking guidance, to covertly gather as much information as possible by attending mosques and community events.<sup>67</sup>

The Supreme Court has recognized that the Fourth Amendment’s protections of private communications are necessary to exercising First Amendment freedoms of speech and association.<sup>68</sup> In enacting FISA, Congress intended to prevent the government from unjustifiably intruding upon the privacy of individuals by providing a means for the government to obtain a warrant before conducting surveillance for intelligence gathering purposes.<sup>69</sup> Thus, by allowing the government to invade the privacy of those the federal government deems to be a “threat,” without a FISA warrant supported by probable cause, we risk chilling the freedom of speech that distinguishes American society from an Orwellian state.<sup>70</sup>

### III. STATE SECRETS

“We’d do well to remember that at the end of the day, the law doesn’t defend us; we defend the law. And when it becomes contrary to our morals, we have both the right and the responsibility to rebalance it toward just ends.” – Edward Snowden

---

<sup>63</sup> See Chesney, *supra* note 61, at 1412 (describing the historical cycle of civil liberties abuse during past times of national security crises).

<sup>64</sup> See *Illusions of Justice*, *supra* note 7, at 18.

<sup>65</sup> *Id.*

<sup>66</sup> American Civil Liberties Union, *ACLU EYE on the FBI: The FBI is Engaged in Unconstitutional Racial Profiling and Racial Mapping* (Oct. 20, 2011), [https://www.aclu.org/files/assets/aclu\\_eye\\_on\\_the\\_fbi\\_alert\\_-\\_fbi\\_engaged\\_in\\_unconstitutional\\_racial\\_profiling\\_and\\_racial\\_mapping\\_0.pdf](https://www.aclu.org/files/assets/aclu_eye_on_the_fbi_alert_-_fbi_engaged_in_unconstitutional_racial_profiling_and_racial_mapping_0.pdf).

<sup>67</sup> See *Illusions of Justice*, *supra* note 7, at 18-19.

<sup>68</sup> *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313-14 (1972).

<sup>69</sup> See SENATE JUDICIARY REPORT, *supra* note 36, at 3908.

<sup>70</sup> See Dawson, *supra* note 26, at 1394.

Where plaintiffs attempt to bring a civil suit on the grounds that they believe they have been warrantlessly surveilled, the government often attempts to bar the suit on the grounds of state secrets privilege.<sup>71</sup> The state secrets privilege is a common law evidentiary privilege that allows the government to prevent discovery of information containing state or military secrets on the basis disclosing such information poses a threat to national security.<sup>72</sup> The privilege can only be invoked by the head of an executive branch agency with the authority to sign a sworn affidavit confirming that he or she has personally reviewed the relevant information and determined it contains state secrets.<sup>73</sup> The state secrets privilege has a long history of invocation,<sup>74</sup> but the government's assertion of the privilege in the post 9/11 era in response to claims of Fourth and First Amendment constitutional violations has led to increasingly unchecked executive power and violations of civil liberties.<sup>75</sup>

The state secrets privilege has origins in the Supreme Court's 1875 decision in *Totten v. United States*.<sup>76</sup> In *Totten*, a Union spy claimed to be in contract with President Lincoln, who told him to travel behind enemy lines and relay information about the Confederate Army in return for \$200 per month.<sup>77</sup> The Court held that it did not have the authority to enforce the contract because the lawsuit would "inevitably lead to the disclosure of matters which the law itself regards as confidential."<sup>78</sup> The very subject matter of the suit, the Court explained, would risk disclosure of "the details

---

<sup>71</sup> Goitein & Patel, *supra* note 31, at 47; see also Laura K. Donohue, *Shadow of States Secrets*, 159 UNIV. PENN. L. REV. 77, 78 (2010).

<sup>72</sup> Stephanie A. Fichera, *Compromising Liberty for National Security: The Need to Rein in the Executive's Use of the State Secrets Privilege in Post-September 11 Litigation*, 62 U. MIAMI L. REV. 625, 628 (2008).

<sup>73</sup> See *Reynolds v. United States*, 345 U.S. 1, 7-8 (1953).

<sup>74</sup> There is some ongoing debate on whether the frequency of the privilege has spiked in the post 9/11 era. Compare Robert M. Chesney, *States Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249, 1301 (2007) (contending that the state's secrets privilege has been invoked with uniform frequency among presidents) with Louis Fisher, *In the Name of National Security: Unchecked Presidential Power and the Reynolds case* 212, 245 (2006) (arguing that the state's secrets privilege is unnecessary, contrary to individual liberties and due process, and supportive of executive abuse of power, asserts that the privilege is being asserted with greater frequency in the post 9/11 era).

<sup>75</sup> Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORDHAM L. REV. 1931, 1938 (2007) ("For over two decades following Reynolds, the executive rarely asserted the state secrets privilege . . . But starting in 1977, the executive raised the privilege with greater frequency"); See also H. R. NO. 110-442, at 8 ("[the current] administration has raised the state secrets privilege in over 25 [percent] more cases per year than previous administrations and sought dismissal in over 90 [percent] more cases.") (citing to 154 Cong. Rec. S198 (daily ed. Jan. 23, 2008) (statement of Sen. Kennedy)).

<sup>76</sup> *Totten v. United States*, 92 U.S. 105 (1875).

<sup>77</sup> *Id.* at 106.

<sup>78</sup> *Id.* at 107.

of dealing with individuals and officers . . . to the serious detriment of the public,” and therefore the Court dismissed the case.<sup>79</sup>

The modern-day state secrets privilege was first announced by the Supreme Court in *Reynolds v. US*.<sup>80</sup> In *Reynolds*, the widows of three men killed in an Air Force B-29 plane crash brought a suit against the United States under the Federal Tort Claims Act.<sup>81</sup> The plaintiffs sought production of the Air Force’s official investigation report and statements of surviving crew members made during the investigation.<sup>82</sup> The Secretary of the Air Force refused to produce the documents, filing a formal claim of state secrets privilege on the grounds that production of the documents would “seriously hamper[ ] national security, flying safety, and the development of highly technical and secret military equipment.”<sup>83</sup> The Supreme Court accepted the government’s claim and held that where there is a formal claim of privilege invoked by the head of an executive department and an indication of a “reasonable possibility that military secrets were involved,” the state secrets privilege may bar disclosure of evidentiary materials.<sup>84</sup> The Court stated that it would be up to the presiding court to determine whether to examine the evidence in question, but forewarned that where there is a danger that evidence will expose matters of national security that should not be disclosed, the court should not “jeopardize the security which the privilege is meant to protect by insisting upon an examination,” even *in camera*.<sup>85</sup>

The executive branch may cite the above two seminal cases in support of a claim of state secrets privilege.<sup>86</sup> The *Totten Bar* applies where the subject matter of the action itself is a state secret.<sup>87</sup> The *Totten Bar* acts as a complete bar on adjudication of claims centered on state secrets.<sup>88</sup> In contrast, the *Reynolds* privilege is an evidentiary tool that acts to remove the privileged evidence from litigation, and only where the state secrets is so interwoven with the case that it cannot be litigated without risk of disclosure is dismissal the proper remedy.<sup>89</sup> Courts have found dismissal under *Reynolds* appropriate in only three circumstances: (1) where the

---

<sup>79</sup> *Id.* at 106-107.

<sup>80</sup> *Reynolds v. United States*, 345 U.S. 1 (1953).

<sup>81</sup> *Id.* at 2-3.

<sup>82</sup> *Id.* at 3; Without the investigation report, the plaintiffs could not establish a prima facie case of negligence, thereby warranting dismissal. *See* Donohue, *supra* note 71, at 82.

<sup>83</sup> *Reynolds*, 345 U.S. at 5.

<sup>84</sup> *Id.* at 4-5, 10-11.

<sup>85</sup> *Id.* at 10.

<sup>86</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1226-28 (9th Cir. 2019) (noting the two instances in which state secrets may apply).

<sup>87</sup> *Id.* at 1227.

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

plaintiff cannot prove their *prima facie* elements of the claim without the privileged evidence; (2) where the privilege deprives the defendant of information needed to put forth a valid defense; and (3) where the privileged evidence is so inextricable with nonprivileged information that is essential to the claims or defenses and litigating a case on its merits would impermissibly risk disclosing state secrets.<sup>90</sup> Despite the clear difference in how the *Totten bar* and *Reynolds* privilege operate to dismiss a case implicating state secrets, the government has practiced moving for outright dismissal of complaints rather than just preclusion of discovery materials since the 1970s.<sup>91</sup>

#### IV. FAZAGA v. FBI

In July 2006, Craig Monteilh began his work as a paid FBI informant targeting the Muslim community in an effort to covertly gather information about Muslims in the Irvine, California area.<sup>92</sup> In an effort to earn the trust of the Muslim community, Monteilh began attending the Islamic Center of Irvine (“ICOI”).<sup>93</sup> Following instructions from his FBI supervisors, he approached an imam,<sup>94</sup> told a fabricated story of his French and Syrian decent and his desire to fully embrace his roots by formally converting to Islam, and from that point forward became entirely immersed in his role as a Muslim convert.<sup>95</sup> Monteilh was provided with surveillance tools, including audio and video recording devices, and was instructed to perform specific spying tasks.<sup>96</sup> These tasks included attending certain meetings and entering the houses of specific people, in order to “gather information on Muslims.”<sup>97</sup> The FBI agents supervising Monteilh made it clear that the FBI had no single target, but instead were interested in the Muslim community as a whole, stating they wanted to “get as many files on this community as possible.”<sup>98</sup>

Over the course of about fourteen months, Monteilh did as instructed by his FBI supervisors to gain the trust of the Muslim community in

---

<sup>90</sup> *Id.* (citing *Mohamed v. Jeppesen Dataplan Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (en banc)).

<sup>91</sup> *Id.* at 1227.

<sup>92</sup> First Amended Complaint, *supra* note 1, at 18.

<sup>93</sup> *Id.*

<sup>94</sup> An Imam is the prayer leader of a mosque. MERRIAM WEBSTER DICTIONARY, <https://www.merriam-webster.com/dictionary/imam>.

<sup>95</sup> *Fazaga*, 916 F.3d at 1212-13.

<sup>96</sup> *Id.*

<sup>97</sup> *Id.*

<sup>98</sup> *Id.* at 1212.

Orange County.<sup>99</sup> Monteilh attended classes at the mosque, collected information on Muslim community members' travel plans, attended daily prayers, exercised with targeted people to build a relationship, visited targeted houses and made lunch plans with specified Muslim individuals.<sup>100</sup> Virtually all of Monteilh's interactions with the Muslim community were recorded with audio and video recording devices, including a cell phone, two key fobs with audio recording capabilities, and a camera disguised as a button on his shirt.<sup>101</sup> Monteilh's recordings included audio from at least eight mosques, video of the layout of various mosques and homes, and most egregiously, conversations and meetings in the mosque prayer hall to which he was not a party to.<sup>102</sup> An electronic device was installed in Fazaga's office and other parts of his mosque not open to the public in order to record these conversations.<sup>103</sup>

Ironically, Operation Flex began to unravel when Monteilh was instructed by his FBI supervisors to press Muslims in the community about jihad and armed conflict. He was told to indicate his readiness to engage in violence, stating he believed it was his "duty as a Muslim to take violent actions" and that he had access to weapons.<sup>104</sup> Several ICOI members took these statements and reported them and Monteilh to community leaders, who then reported Monteilh to the FBI.<sup>105</sup> The IOCI obtained a restraining order against Monteilh in June 2007, around the same time the FBI discharged him from Operation Flex.<sup>106</sup> The dragnet surveillance did not result in a single counterterrorism conviction—a predictable result considering the FBI targeted the Muslim community based solely on their religious practice and not on the basis of any suspected criminal activity.<sup>107</sup>

In September 2011, Plaintiffs filed suit as a putative class action on behalf of "[a]ll individuals targeted by Defendant for surveillance or information-gathering through Monteilh and Operation Flex, on the account of their religion, and about whom the FBI gained personally identifiable information."<sup>108</sup> The complaint alleged eleven causes of action, which can be categorized as claims alleging unconstitutional searches in violation of the Fourth Amendment and claims alleging illegal discrimination on the basis of, or burdens on, or abridgement of religion

---

<sup>99</sup> *Id.* at 1213.

<sup>100</sup> *Id.* at 1212-13.

<sup>101</sup> *Id.* at 1213.

<sup>102</sup> *Id.*

<sup>103</sup> *Id.*

<sup>104</sup> *Id.* at 1213-14.

<sup>105</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1214 (9th Cir. 2019).

<sup>106</sup> *Id.*

<sup>107</sup> First Amended Complaint, *supra* note 1, at 1.

<sup>108</sup> *Fazaga*, 916 F.3d at 1214.



in violation of the First Amendment.<sup>109</sup> Plaintiffs sought injunctive relief, specifically an order for Defendants to destroy or return any information gathered by or derived from the unlawful surveillance program, as well as damages, for themselves and the class.<sup>110</sup> The government moved to dismiss and for summary judgment on the grounds that the religion claims—but not the search claims—should be dismissed under the *Reynolds* state secrets privilege because litigation on those claims could not go forth without the threat of disclosure of evidence protected by state secrets.<sup>111</sup>

The district court’s first order dismissed the FISA claim against the government, but not the agent Defendants, on the basis that Congress had not waived sovereign immunity under FISA.<sup>112</sup> In a second order, the district court dismissed all claims asserted by Plaintiffs on the basis of *Reynolds* state secrets privilege, including the Fourth Amendment search claims, which the Government did not seek dismissal of on state secrets grounds.<sup>113</sup> The district court held that the subject matter of the action, Operation Flex, “involved intelligence that, if disclosed, would significantly compromise national security.”<sup>114</sup> The district court found that the Government Defendants would need to rely on privileged evidence “so inextricably tied up with nonprivileged material” that the risk of disclosure could not be averted through protective procedures.<sup>115</sup> The district court also declined to use the *in camera*, *ex parte* procedures provided under §1806(f) of FISA, concluding that FISA’s procedures do not apply to non-FISA claims.<sup>116</sup>

The Ninth Circuit reversed the district court’s dismissal of Plaintiffs’ claims on state secrets grounds.<sup>117</sup> The court, relying on Fourth Amendment caselaw and paying careful attention to First Amendment implications, found that the plaintiffs pleaded plausible FISA claims.<sup>118</sup>

---

<sup>109</sup> *Id.* at 1214, 1235.

<sup>110</sup> *Id.* at 1214.

<sup>111</sup> *Id.* at 1214-15. The other defendants, who are all Agents of the FBI being sued in their official capacity, moved to dismiss claims against them on multiple grounds, including qualified immunity. Because those defenses present issues separate from the central issue in this note, they will not be discussed.

<sup>112</sup> *Id.* at 1215.

<sup>113</sup> *Id.*

<sup>114</sup> *Id.*

<sup>115</sup> *Id.*

<sup>116</sup> *Id.*

<sup>117</sup> *Id.* at 1254.

<sup>118</sup> *Id.* at 1253-54. The court found some of the FISA claims were not plausible because the Plaintiffs lacked an expectation of privacy under Fourth Amendment caselaw, and some of the claims were plausible but the agents were entitled to qualified immunity because the law was unclear. Because this note focuses on the FISA claims that were allowed to proceed, these holdings will not be discussed in depth.

The court held the procedures established by Congress in FISA replaced the dismissal remedy to common law state secrets privilege as applied to electronic surveillance.<sup>119</sup> The court noted that the district court erred in dismissing some of the claims outright on state secrets grounds where the government did not assert the privilege, and on the claims in which the government *did* assert the privilege, the district court should have reviewed any state secrets evidence necessary for a determination of whether the surveillance was illegal pursuant to FISA procedures.<sup>120</sup> In a ruling of first impression, the court reaffirmed the legislative intent behind FISA, emphasizing Congress's aim at reigning in executive abuse of electronic surveillance.<sup>121</sup> The court held that FISA's §1806(f) procedures applied to affirmative constitutional challenges to unlawful surveillance or its use in litigation, regardless of whether the challenge is brought under FISA, the Constitution, or any other law.<sup>122</sup>

## V. ANALYSIS

The Ninth Circuit in *Fazaga v. FBI* revived the purpose of FISA, and in doing so, upheld the basic constitutional principles of separation of powers. First, the court correctly analyzed the FISA claims under a traditional—yet scrupulous—Fourth Amendment analysis, using *Katz*'s reasonable expectation of privacy test and acknowledging the implications of First Amendment rights in national security cases like this one. Second, the court properly held that the procedures established by Congress in FISA were intended to displace the state's secrets privilege in so far as it called for outright dismissal of claims.

### a. *The Court Justifiably Applied Careful Fourth Amendment Analysis*

“The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of individuals. Power is a heady thing; and history shows that the police acting on their own cannot be trusted.” – *McDonald v. US* (1948)

The *Fazaga* court was correct in scrupulously analyzing the Plaintiffs' expectations of privacy in this context because much of the privacy

---

<sup>119</sup> *Id.* at 1233-34.

<sup>120</sup> *Id.* at 1211 (emphasis added).

<sup>121</sup> *Id.* at 1225, 1233.

<sup>122</sup> *Id.* at 1238.

violations took place in a religious setting and thus implicated both First and Fourth Amendment rights.<sup>123</sup> After determining the complaint sufficiently pleaded that Plaintiffs were “aggrieved persons” as defined by FISA, the court then turned to whether the surveillance in Operation Flex constituted “electronic surveillance” within the meaning of FISA.<sup>124</sup> The court explained that in order for the defendant’s electronic surveillance to constitute a violation under FISA, the court must find that (1) plaintiffs had a reasonable expectation of privacy, and (2) a warrant would be required for law enforcement purposes.<sup>125</sup>

#### i. The Reasonable Expectation of Privacy Analysis Under FISA is the Same as Under the Fourth Amendment

FISA provides for criminal sanctions and civil liability where law enforcement undertakes electronic surveillance without a FISA warrant in situations where there exists a “reasonable expectation of privacy.”<sup>126</sup> The court properly analyzed the statutory “reasonable expectation of privacy” standard analogously to the analysis under traditional law enforcement purposes because the origins of FISA can be traced back to executive branch’s unconstitutional electronic surveillance for law enforcement purposes.<sup>127</sup> The decision in *Katz* rejected the proposition that the executive branch has unlimited power to conduct electronic surveillance for law enforcement purposes without prior judicial approval.<sup>128</sup> The *Katz* reasonable expectation of privacy standard has since been named the “touchstone of Fourth Amendment analysis.”<sup>129</sup> The legislature followed the court’s cue in *Katz* by creating the Wiretap Act, which allows law

---

<sup>123</sup> See *infra* Part IV.a.

<sup>124</sup> *Fazaga*, 916 F.3d at 1216, 1239. FISA provides four categories of electronic surveillance. See *supra* note 40, and accompanying text. In this case, only the fourth category was at issue: “the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.” 50 U.S.C. § 1801(f)(4).

<sup>125</sup> *Fazaga*, 916 F.3d at 1217 (noting that the complaint alleges no warrant was obtained, the court’s analysis focused on whether plaintiffs had a reasonable expectation of privacy).

<sup>126</sup> 50 U.S.C. §§ 1801(f), 1809-10.

<sup>127</sup> See *supra* Part III and accompanying text discussing the origins of FISA as dating back to *Olmstead* and *Katz*.

<sup>128</sup> *Katz v. United States*, 389 U.S. 347, 359 (1967).

<sup>129</sup> *California v. Ciraolo*, 47 U.S. 207, 211-212 (1986).

enforcement to conduct electronic surveillance only with prior judicial approval in the form of Title III warrants.<sup>130</sup>

Likewise, the enactment of FISA was a reaction by Congress to executive abuse of power in the form of electronic surveillance in the name of “national security” in much the same respect as the Wiretap Act was a reaction the same form of executive abuse in the name of law enforcement.<sup>131</sup> Insofar as FISA originates from a desire to protect the Fourth Amendment’s guarantee to be free from unreasonable governmental intrusions, the court in *Fazaga* correctly evaluated the statutory standard of “reasonable expectation of privacy” in FISA just as the expectation of privacy standard would be under the Fourth Amendment for law enforcement purposes.

#### ii. Plaintiffs Expectations of Privacy are Greater in Religious Spaces

In determining whether or not Plaintiffs had a reasonable expectation of privacy, the court exhibited a heightened level of skepticism towards the executive branch where Plaintiffs’ freedom of religion was also implicated.<sup>132</sup> The court did so by separating the instances of surveillance where there was a religious characteristic of the surveilled activity.<sup>133</sup> First, in accordance with traditional Fourth Amendment caselaw,<sup>134</sup> the court held that Plaintiffs did not have a reasonable expectation of privacy for recordings of conversations in which Monteilh was a party, therefore no violation of FISA occurred.<sup>135</sup> This is because where an undercover agent is an “invited informer,” Plaintiffs do not have a privacy interest in what is voluntary revealed to that agent.<sup>136</sup> Nonetheless, the court found that under well-established Fourth Amendment caselaw, there is a reasonable expectation of privacy from covert recordings of conversations taking

---

<sup>130</sup> See Whilt, *supra* note 25, at 371 (“Congress enacted Title III, a statute governing electronic surveillance modeled after constitutional guidelines specified by the Supreme Court in *Katz*”).

<sup>131</sup> See Dawson, *supra* note 26, at 1386-87.

<sup>132</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1244 (9th Cir. 2019).

<sup>133</sup> *Id.* at 1218, 1222.

<sup>134</sup> *Fazaga*, 916 F.3d at 1219 (citing *United States v. Walchumwah*, 710 F.3d 862, 867 (9th Cir. 2013) (citing the invited informer doctrine for the proposition that voluntary conversations with undercover informants are not protected by the Fourth Amendment because voluntary disclosures lack reasonable expectations of privacy); see generally Mike Bothwell, *Facing God or the Government—United States v. Aguilar: A Big Step for Big Brother*, 1990 BYU L. REV. 1003 (1990) (discussing the invited former doctrine and its impingement on first and Fourth Amendment constitutional rights).

<sup>135</sup> *Fazaga*, 916 F.3d at 1220.

<sup>136</sup> *Id.* at 1219.

place in one's home, car, office, or phone.<sup>137</sup> Because there was evidence FBI agents bugged Plaintiff Fazaga's office and Plaintiff AbdelRahim's house,<sup>138</sup> and no warrant was obtained, these recordings plausibly alleged a violation of FISA.<sup>139</sup>

The court justifiably applied more careful Fourth Amendment analysis where the recordings took place in sacred religious spaces, such as the Mosque prayer halls. A reasonable expectation of privacy involves two inquiries: first, that the person had a subjective expectation, and second, the expectation of privacy is one that society is prepared to accept.<sup>140</sup> When First Amendment expressions of religion, especially in private places, are involved, there exists an unquestionable expectation of the exact privacy the Fourth Amendment was intended to protect.<sup>141</sup> The expression of private thoughts, prayers, and confessions, relies on the ability to trust one is not being overheard.<sup>142</sup>

In *Katz*, the Supreme Court emphasized the subjective intent to be free of eavesdropping intruders, exhibited by shutting the door to a telephone booth.<sup>143</sup> Here, the court in *Fazaga* found that "based on the rules and customs of the mosque, and the allegations in the complaint," it had "no trouble determining that Plaintiffs manifested an actual, subjective expectation of privacy in their conversations there."<sup>144</sup> The court emphasized that the mosque was not an ordinary space—it is a place of worship, prayer, and fellowship.<sup>145</sup> Moreover, the ICOI—where many Plaintiffs attended—specifically forbade audio or video recording in the mosque without permission.<sup>146</sup> Thus, the court correctly held that Plaintiffs exhibited a subjective expectation of privacy in their activities within the mosque prayer hall.

---

<sup>137</sup> *Id.* at 1224.

<sup>138</sup> *Id.* at 1225 (including a statement by FBI agents questioning Monteilh for not disclosing a conversation that occurred in AbdelRahim's house and that they knew of the conversation because of the recordings).

<sup>139</sup> *Id.*

<sup>140</sup> *California v. Ciralo*, 476 U.S. 207, 211 (1986).

<sup>141</sup> *See supra* note 36; *See also* *United States vs. United States Dist. Ct. (Keith)*, 407 U.S. 297, 313-14 (1972).

<sup>142</sup> *See* Michael Avery, *The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States*, 62 U. MIAMI L. REV. 541, 597 (2008).

<sup>143</sup> *See Katz v. United States*, 389 U.S. 347, 352 ("[A] person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it . . . is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

<sup>144</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1220 (9th Cir. 2019).

<sup>145</sup> *Id.* at 1220.

<sup>146</sup> *Id.* at 1221.

The court properly rejected the government's argument that because Plaintiffs were not alone, their expectation of privacy was diminished.<sup>147</sup> As the court explained, a person is entitled to have an expectation of privacy in shared spaces, especially where there is a particular reason to expect confidentially.<sup>148</sup> Moreover, the Supreme Court has held that whether a space is shared does not diminish the expectation that a person will not be *recorded* in that space.<sup>149</sup> Mosques *specifically* are a place where trust and confidence is essential, because much of the discussion revolves around theology and the practice of Islam.<sup>150</sup> The court was therefore correct to find that Plaintiffs had a subjective intent to express their religious beliefs and exchange ideas and emotions in a safe space, free from government observation.

After finding that Plaintiffs exhibited a subjective expectation of privacy, the court correctly determined that Plaintiffs had an expectation of privacy that society was prepared to recognize as reasonable.<sup>151</sup> The court highlighted that context is key to this inquiry, and thus emphasis should be placed on the nature of the place where the recordings were made.<sup>152</sup> Here, the mosque prayer hall is a sacred and intimate place that is distinguishable from typical public spaces.<sup>153</sup> The court accurately emphasized the location of the Mosque prayer hall, because the Fourth Amendment requires that sight is not lost of the place in which a person expects privacy.<sup>154</sup> For example, the framers designed the warrant clause of the Fourth Amendment to require particularity with respect to the place to be searched in order to protect private spaces and permit searches only where evidence of a crime may be found.<sup>155</sup> The Constitution's intentional limitations on law enforcement's ability to search particular spaces without a warrant confirms that some spaces are objectively more private than others.<sup>156</sup> The court skillfully contrasted the sacred nature of the mosque prayer hall with public spaces where society accepts a diminished

---

<sup>147</sup> *Id.*

<sup>148</sup> *Id.*

<sup>149</sup> *Id.* at 1221-22 (*citing* *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018)).

<sup>150</sup> *Fazaga*, 916 F.3d at 1221.

<sup>151</sup> *Id.* at 1223.

<sup>152</sup> *Id.* at 1222.

<sup>153</sup> *Id.*

<sup>154</sup> *See Avery*, *supra* note 141, at 596-97.

<sup>155</sup> *Id.*; U.S. CONST. amend. IV. ("No Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.")

<sup>156</sup> Another example is the home. Although there are many exceptions to the warrant requirement in public spaces, such as exigent circumstances, the Supreme Court has repeatedly found that searches and seizures inside of a home are assumed to be unreasonable. *See, e.g., Brigham City, Utah v. Stuart*, 126 S. Ct. 1943, 1947 (2006).

sense of privacy, finding that the judiciary’s “constitutional protection of religious observance” supports finding a reasonable expectation of privacy in the mosque prayer hall where privacy concerns are recognized and protected.<sup>157</sup>

Finally, the court underscored the First Amendment implications of the mosque prayer hall on Fourth Amendment expectations of privacy.<sup>158</sup> Relying on Supreme Court caselaw, the court explained that when the surveillance is aimed at content protected by the First Amendment, “the Fourth Amendment must be applied with ‘scrupulous exactitude.’”<sup>159</sup> True enjoyment of First Amendment freedoms cannot take place without Fourth Amendment protections—the growth of self, the finding of theological values, and even reflections of political dissent rely on the ability to trust one will be left alone.<sup>160</sup> Particularly for Muslims, prayer is a pillar of religion: it is a necessary and profound ritual that requires individual devotion and expungement of the outside world.<sup>161</sup> This sacred religious practice, therefore, cannot exist without the ability to be free of unwanted observations.<sup>162</sup> The court recognized the prayers and religious activities that Operation Flex targeted were of the kind of activities that the Fourth Amendment was drafted, in part, to protect and must be considered reasonable.<sup>163</sup>

The Supreme Court has long recognized that national security cases comprise an extraordinary merging of First and Fourth amendment values.<sup>164</sup> Given that the Supreme Court has already rejected the executive’s use of warrantless surveillance in domestic security cases, finding that “unreviewed executive discretion” may too readily “overlook potential *invasions of privacy and protected speech*,”<sup>165</sup> it was only suitable for the court in *Fazaga* to recognize these same Fourth and First Amendment concerns also exist in foreign security cases. This is especially true following the 9/11 attacks, in which time there has been a

---

<sup>157</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1223 (9th Cir. 2019).

<sup>158</sup> *Id.*

<sup>159</sup> *Id.* (internal quotation marks omitted).

<sup>160</sup> *See Avery*, *supra* note 141, at 588; *see also Olmstead v. United States*, 277 U.S. 478 (1928) (Brandeis, J., dissenting) (arguing that the Framers of the Constitution, in writing the Fourth Amendment, “conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.”).

<sup>161</sup> *See The Five Pillars of Islam*, METRO. MUSEUM OF ART, <https://www.metmuseum.org/learn/educators/curriculum-resources/art-of-the-islamic-world/unit-one/the-five-pillars-of-islam>; *see also Worship*, BBC, <https://www.bbc.co.uk/bitesize/guides/z94dtfr/revision/1>.

<sup>162</sup> *See Avery*, *supra* note 141, at 597.

<sup>163</sup> *Id.* at 596-97.

<sup>164</sup> *United States v. United States Dist. Ct. (Keith)*, 407 U.S. 297, 313 (1972).

<sup>165</sup> *Id.* at 317 (emphasis added).

rise in abridgments of First Amendment rights of Muslims in America.<sup>166</sup> Here, where Plaintiffs were targeted on the sole basis of their religious associations, the court was right to recognize that Fourth Amendment protections become “more necessary when the targets of official surveillance may be those suspected of unorthodoxy.”<sup>167</sup> After all, FISA itself serves as congressional recognition that Fourth Amendment rights must not be abridged on the basis of First Amendment protected freedoms, such as religious expression.<sup>168</sup> Accordingly, the court was justified in concluding that society recognizes an expectation of privacy, perhaps worthy of even greater Fourth Amendment protections, where freedom of religious expression is at stake.<sup>169</sup>

*b. The Court Reinforced Separation of Powers Principles in Holding FISA Procedures Overruled the State’s Secrets Dismissal Remedy*

In holding that Plaintiffs’ claims could proceed through the tailored procedures Congress established in FISA, the court upheld basic principles of constitutional separation of powers and checks and balances. The court emphasized the legislative intent behind FISA: to provide a check on the executive’s abusive use of electronic surveillance in the name of national security.<sup>170</sup> In doing so, the court accomplished three very important aims. First, the court prevented the executive branch from transforming the *Reynolds* evidentiary privilege into a broad claim of executive immunity. Second, the court confirmed Congress’s intent to delegate to the judiciary branch a role in checking on the executive branch’s encroachment on civil liberties under the guise of national security. Finally, the court fulfilled its constitutional duty to oversee executive action where an individual alleges abuse of authority, unconstitutional conduct, or violation of a statute.

---

<sup>166</sup> See generally *Illusions of Justice*, *supra* note 7.

<sup>167</sup> *United States v. United States Dist. Ct. (Keith)*, 407 U.S. at 314.

<sup>168</sup> See S. REP. NO. 95-604(I), 1978 U.S.C.C.A.N. 3904, 3908 (“The exercise of political freedom depends in large measure on citizen’s understanding that they will be able to be publicly active and dissent from official policy . . . without having to sacrifice the expectation of privacy that they rightfully hold.”).

<sup>169</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1224 (9th Cir. 2019) (concluding that although the plaintiffs had a reasonable expectation of privacy in their conversations within the Mosque prayer halls, the law was unclear in the area and so the FBI Agent Defendants were entitled to qualified immunity for this category of recordings).

<sup>170</sup> *Id.* at 1233.



i. The Court Correctly Affirmed that Reynolds is a Rule of Evidence, Not a Constitutional Construction for Unitary Executive Power

As the court explained, the *Reynolds* privilege is an evidentiary rule evolved through common-law, it is not a constitutional instrument for the executive to claim unchecked, arbitrary power.<sup>171</sup> The state secrets privilege, if left unbound, has the ability to shield the executive from accountability, public scrutiny, and potential civil liability by removing judicial review and preventing abuses of power from coming to light through litigation.<sup>172</sup> Moreover, the privilege has the power to turn a limited evidentiary rule into a constitutional claim of unitary executive power over any and all claims pertaining to national security.<sup>173</sup> Where the privilege is used to outright dismiss cases—especially at the pleading stage before discovery—the executive immediately insulates himself from judicial and public scrutiny, over time transforming the privilege into a tool for concentrating power in one branch.<sup>174</sup>

Ironically, the devastating consequences of the state secrets privilege on constitutional guarantees are exactly why it was necessary for the court to pronounce that the state secrets privilege is not a rule of constitutional construction—it is a rule of evidence.<sup>175</sup> By reciting the common-law origins of the privilege and the limited situations in which the *Reynolds* privilege may serve to dismiss a case, the court rejected the executive's claim that the privilege may act as unbound deference through which executive defendants may insulate themselves.<sup>176</sup> Indeed the *Reynolds* court itself recognized the court's gatekeeping function for the state's privileged evidence, instructing the court to determine itself whether the claim of privilege was appropriate under the circumstances, while being careful not to disclose national security secrets. As the *Fazaga* court noted, however, a mere cry of military secrets, counterterrorism, or national security by the executive is not sufficient to support a finding that the evidence is privileged. Instead, courts should continue to act as the gatekeepers of evidence, even where state secrets are at stake, to avoid being over deferential to the executive and disrupting separation of powers principles.<sup>177</sup> Finally, by confining the state secrets privilege, and the

<sup>171</sup> *Id.* at 1231.

<sup>172</sup> See Fichera, *supra* note 72, at 627.

<sup>173</sup> See Frost, *supra* note 75, at 1932; see also Fichera, *supra* note 72, at 640.

<sup>174</sup> See Chesney, *supra* note 74, at 1269.

<sup>175</sup> *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1231 (9th Cir. 2019).

<sup>176</sup> *Id.* at 1227.

<sup>177</sup> See Fisher, *supra* note 74, at 258 (“Broad deference by the courts to the executive branch, allowing an official to determine what documents are privileged, undermines the judiciary’s duty to assure fairness in the courtroom and to decide what evidence may be

*Reynolds* rule in particular, to a common law rule of evidence rather than constitutional construction, the court gave constitutional support to Congress's ability to overrule state secrets through the legislation of FISA.<sup>178</sup>

After the court reiterated the common-law nature of the state secrets privilege and confirmed Congress's ability to legislate over the privilege,<sup>179</sup> the court's holding confirmed Congress's intent to make §1806(f) of FISA the *exclusive means* for evaluating evidence that potentially threatens national security in determining the legality of electronic surveillance.<sup>180</sup> The court explained that the procedures in §1806(f) arise from the same concern as the state secrets privilege—disclosure of evidence that threatens national security—and that §1806(f) is triggered in a nearly identical process to the formal assertion triggering state secrets privilege.<sup>181</sup> As such, the court concluded that §1806(f) codified the state secrets privilege with respect to consideration of electronic state secrets evidence, directing *in camera* and *ex parte* review of the relevant evidence in place of the common law dismissal remedy.<sup>182</sup> By ruling FISA procedures to eliminate the need for *Reynolds* dismissal remedy, the court reduces the executive's ability to insulate himself from scrutiny by claiming broad governmental immunity.

#### ii. The Court Accepted Congress's Invitation to Provide a Constitutionally Granted Joint Check on the President

The court found that the legislative intent behind FISA supports the conclusion that Congress intended to give the courts a role in regulating foreign intelligence surveillance.<sup>183</sup> FISA was a response to the executive's abusive surveillance practices in the name of national security, which lead to violations of constitutional rights of citizens "primarily

---

introduced." For a further discussion of the Judiciary Branch's constitutional duties, see *infra* part V.B.iii.

<sup>178</sup> *Fazaga*, 916 F.3d. at 1231-32.

<sup>179</sup> The court briefly noted that a clear statement by Congress that it was overruling a common law rule is not required, only that the legislation "speaks directly to the question" otherwise answered by federal common law is required. Here, the court found the procedures in 1806(f) of FISA spoke directly to the dismissal remedy otherwise available under common law state secrets privilege. *Id.* at 1231.

<sup>180</sup> § 1806(f) provides that where a motion is made to suppress evidence relating to electronic surveillance on the grounds that disclosure would harm national security, the district court hearing the motion should review *in camera* and *ex parte* the evidence to determine whether the surveillance was lawfully authorized and conducted. 50 U.S.C. § 1806(f); see also *Fazaga*, 926 F.3d at 1231.

<sup>181</sup> *Fazaga*, 916 F.3d at 1232.

<sup>182</sup> *Id.* at 1231-32.

<sup>183</sup> *Id.* at 1232.

because checks and balances designed by the framers of the Constitution to assure accountability [were not] applied.”<sup>184</sup> The court aptly highlighted that FISA strikes a balance by enlisting both Congress and the courts in the oversight of surveillance activities by the executive branch while providing measures to safeguard national security.<sup>185</sup> The court noted that Congress considered the limitations placed on the courts under the common law state secrets privilege, and intentionally recruited the courts in protecting against electronic surveillance by enacting FISA.<sup>186</sup>

The court’s endorsement of FISA’s careful system of checks on broad executive claims of state secrets reaffirmed the framers’ will that each branch of government shall play a role in checking on the others, so that no one branch usurps power from the other branches.<sup>187</sup> The framers feared the abuse of executive power most, which is why the separation of powers acts as a failsafe by allowing Congress to enjoin the court in checking on the executive’s actions.<sup>188</sup> Congress is empowered to delegate when the courts should provide a check on the executive by granting them jurisdiction to hear a variety of cases.<sup>189</sup> When courts acquiesce to the executive’s attempt to dismiss cases on the grounds that evidence is protected by state secrets privilege, the court undermines Congress’s attempt to cooperate with the courts, leaves the executive unchecked by any branch, and jeopardizes civil liberties.<sup>190</sup>

---

<sup>184</sup> *Id.* at 1233 (citing S. REP. NO. 94-755, at 289 (1976)).

<sup>185</sup> *Id.* at 1232 (citing *In re NSA Telecomms. Records Litig.*, 564 F. Supp. 2d 1109, 1119 (N.D. Cal. 2013)); see also Ira S. Shapiro, *The Foreign Intelligence Act: Legislative Balancing of National Security and the Fourth Amendment*, 15 HARV. J. ON LEGIS. 119, 204 (“In place of the lawlessness of the past, [FISA] offers a system of internal executive accountability, a meaningful, antecedent role for the courts, consistent with the Fourth Amendment . . .”).

<sup>186</sup> *Fazaga*, 916 F.3d at 1233-34. See Frost, *supra* note 75, at 1957 (“Congress’s deliberate use of the courts as a check on abuse of executive power should be a factor in the court’s analysis of the state secrets privilege. Courts should always be cautious when faced with executive assertion of the privilege, but they should be especially reluctant to dismiss entire categories of challenges to executive actions that Congress intended them to hear.”).

<sup>187</sup> See also Erwin Chemerinsky, *The Assault on the Constitution: Executive Power and the War on Terrorism*, 40 U.C. DAVIS L. REV. 1, 16-17 (2006) (stating checking executive power is “a central goal of the American constitution. [. . .] [t]he framers of the Constitution feared executive power the most [and therefore] viewed the principle of separation of powers as the central guarantee of a just government.”).

<sup>188</sup> *Id.*; see Frost, *supra* note 75, at 1933.

<sup>189</sup> See Frost, *supra* note 75, at 1951, 1932 n.5 (noting that 28 U.S.C. § 1331 grants courts jurisdiction to hear all civil actions “arising under” federal law).

<sup>190</sup> See Frost, *supra* note 75, at 1933; see also Fisher, *supra* note 74, at 262 (“The Framers adopted separation of powers and checks and balances because they did not trust human nature and feared concentrated power. To defer to agency claims about privileged documents and state secrets is to abandon the independence that the Constitution vests in

The Ninth Circuit in *Fazaga* simply applied these principles to find that Congress intended FISA to delegate to the courts authority to check the executive where claims of unconstitutional surveillance arise.<sup>191</sup> In doing so, the court accepted the legislature's offer to join forces in keeping the executive's surveillance practices in line with the constitution. The court's claim of authority is significant because the alliance between the legislative and judicial branch becomes all the more important where, as here, the civil liberties at stake are plenty and depend on the constitutional guarantee of checks and balances.<sup>192</sup>

### iii. The Court Fulfilled the Constitutional Duties of the Judiciary Branch

The court in *Fazaga* executed its constitutional duty to oversee claims of illegal executive action and provide redress where constitutional rights are violated.<sup>193</sup> The executive often uses the claim of privilege to strip judicial power to oversee executive action.<sup>194</sup> Were the courts to give the executive broad, unquestioned deference in determining what evidence contains state secrets and therefore must be privileged, there will be no role left for the judiciary to oversee fairness in litigation and determine what evidence may be introduced.<sup>195</sup> As one constitutional scholar has put it, if the judicial branch "rarely if ever actually reject[s] an assertion of the privilege, a perception may arise within the executive branch . . . that judicial review has no true bite . . ." <sup>196</sup> *Fazaga* therefore put the "bite" back in judicial review by confirming the courts' jurisdiction to hear cases challenging the constitutionality of foreign intelligence surveillance. Finally, by not being over deferential to the executive branch's claim of state secrets, the court faithfully effected its constitutional duties to uphold the laws of the land and provide redress where individual rights are abridged.

---

Congress and the courts, placing in jeopardy the individual liberties that depend on institutional checks.").

<sup>191</sup> *Fazaga*, 916 F.3d at 1231.

<sup>192</sup> See Fichera, *supra* note 72, at 641.

<sup>193</sup> "[I]t is the federal courts' role to restrain and remedy unconstitutional government conduct, and separation of powers is enhanced, not infringed, when the judiciary hears and decides constitutional cases." Erwin Chemerinsky, *FEDERAL JURISDICTION* 34-35 (4th ed. 2003).

<sup>194</sup> See Frost, *supra* note 75, at 1956-67.

<sup>195</sup> *Id.* at 1950-51.

<sup>196</sup> See Chesney, *supra* note 74, at 1311.

## VI. CONCLUSION

Technology has given the individual great freedom to relax by solving much of life's inconveniences. At the same time, technology has put civil liberties at great risk in a world where tiny recording devices can be found and obtained with a quick search on Amazon.<sup>197</sup> Today in the wake of the Edward Snowden leaks, the sale of consumer information by social networks, and dragnet FBI surveillance, it is clear the consequences our precious electronics may have on our right to privacy have only grown since the enactment of FISA. If Americans are to retain any meaningful right to privacy, and corollary right to freedom of expression within that realm of privacy, checks and balances must remain in place to prevent repetitive executive abuse of power. The Ninth Circuit's use of FISA as a tool of separation of powers reflects a courageous willingness of the judicial branch to engage in checking executive function where core civil liberties are at stake. While cries of national security threats are often used to incite fear, America would do well to keep a watchful eye on the biggest threat to our civilized democracy—an unbound executive chipping away at civil liberty.

---

<sup>197</sup> Search results for "small recording device," AMAZON.COM, <https://www.amazon.com> (search in search bar for "small recording device").